V. M. Sidel'nikov, S. O. Shestakov, On an encoding system constructed on the basis of generalized Reed–Solomon codes, *Diskr. Mat.*, 1992, Volume 4, Issue 3, 57–63

Дискретная математика

том 4 выпуск 3 * 1992

УДК 519.72

О СИСТЕМЕ ШИФРОВАНИЯ, ПОСТРОЕННОЙ НА ОСНОВЕ ОБОБЩЕННЫХ КОДОВ РИДА–СОЛОМОНА

В.М. Сидельников, С.О. Шестаков

В работах [1, 2] на базе теоретико-кодовых конструкций предложены методы построения системы открытого шифрования. Их основой является общеизвестная матрица $\mathfrak{B}$ размера $s+1 \times N$ с элементами из конечного поля $\mathbf{F}_q$ вида $\mathfrak{B} = H \cdot \mathfrak{A}$, где $\mathfrak{A}$ – некоторая неизвестная матрица, являющаяся проверочной матрицей q-значного обобщенного кода Рида–Соломона кода (ОРС-код), в частности, кода Гоппы, а H – неизвестная невырожденная матрица размеров $s+1 \times s+1$.

В настоящей работе предложен метод нахождения неизвестных матриц $\mathfrak{A}, H$ с элементами из поля $\mathbf{F}_q$, который определяют матрицу $\mathfrak{B}$, за $O(s^4 + sN)$ операций. Тем самым устанавливается ненадежность рассматриваемых систем открытого шифрования.

§ 1. Описание системы открытого шифрования

Рассмотрим систему "открытого шифрования", предложенную в [2], применительно к ОРС-кóду $\mathbf{K}$. Пусть $\mathbf{F}_q$ – конечное поле, содержащее q элементов, и $\mathbf{F} = \mathbf{F}_q \cup \infty$ – поле, к которому добавлен элемент ∞, обладающий естественными свойствами. Рассмотрим матрицу $\mathfrak{A}$ с элементами из $\mathbf{F}_q$ вида

$$\mathfrak{A}(\alpha_1, \ldots, \alpha_N; z_1, \ldots, z_N) = \left\| \begin{matrix} z_1\alpha_1^0 & z_2\alpha_2^0 & \ldots\ldots & z_N\alpha_N^0 \\ z_1\alpha_1^1 & z_2\alpha_2^1 & \ldots\ldots & z_N\alpha_N^1 \\ \multicolumn{4}{c}{\dotfill} \\ z_1\alpha_1^s & z_2\alpha_2^s & \ldots\ldots & z_N\alpha_N^s \end{matrix} \right\|, \tag{1}$$

где $\alpha_i \in \mathbf{F}$, $z_i \in \mathbf{F}_q \backslash \{0\}$, $\alpha_i \neq \alpha_j$ при $i \neq j$ и при $\alpha_j = \infty$ соответствующий столбец имеет вид $z_j(0, \ldots, 0, 1)^T$. Матрица $\mathfrak{A}$ является проверочной матрицей q-значного кода $\mathbf{K} = \mathbf{K}(\mathfrak{A})$ длины N, который является (укороченным при $N < q+1$) ОРС-кодом (см. [3]). Пусть $\mathfrak{E}$ – ансамбль, состоящий из всевозможных матриц вида $\mathfrak{B} = H \cdot \mathfrak{A}$, где матрица $\mathfrak{A}$ пробегает множество всех матриц вида (1), а H – множество невырожденных матриц с элементами из поля $\mathbf{F}_q$ размера $s+1 \times s+1$. Из определений вытекает, что любая матрица $\mathfrak{B}$ ансамбля $\mathfrak{E}$ имеет вид

$$\mathfrak{B} = \left\| \begin{matrix} z_1 f_1(\alpha_1) & z_2 f_1(\alpha_2) & \ldots & z_N f_1(\alpha_N) \\ z_1 f_2(\alpha_1) & z_2 f_2(\alpha_2) & \ldots & z_N f_2(\alpha_N) \\ \multicolumn{4}{c}{\dotfill} \\ z_1 f_{s+1}(\alpha_1) & z_2 f_{s+1}(\alpha_2) & \ldots & z_N f_{s+1}(\alpha_N) \end{matrix} \right\|, \tag{2}$$

где многочлены $f_j(x)$ степени не выше s линейно независимы над полем $\mathbf{F}_q$ и определяются очевидным образом матрицей H.

Коротко опишем систему "открытого шифрования", основанную на идеях работы [2]. В этой системе абонент $\mathfrak{X}$ случайно и равновероятно выбирает в ансамбле $\mathfrak{E}$ матрицу $\mathfrak{B}$ вида (2). Матрица $\mathfrak{B}$ является общедоступной, а матрицы H и $\mathfrak{A}$ держатся абонентом $\mathfrak{X}$ в секрете. Сообщение B, передаваемое абонентом η и предназначенное абоненту $\mathfrak{X}$, передается по общедоступному каналу связи и представляет собой столбец $B = \mathfrak{B} \cdot \bar{a}$, где вектор $\bar{a}$ длины N содержит не более $t = [s/2]$ ненулевых координат, принимающих значение в поле $\mathbf{F}_q$. Вектор $\bar{a}$ содержит конфиденциальную информацию абонента η, предназначенную для перечади абоненту $\mathfrak{X}$. Абонент $\mathfrak{X}$, получив вектор-столбец B и зная матрицы H и $\mathfrak{A}$, может "достаточно быстро", используя один один из известных алгоритмов декодирования ОРС-кода, восстановить вектор $\bar{a}$. Если матрицы H и $\mathfrak{A}$ неизвестны, то восстановление вектора $\bar{a}$ представляет собой "сложную проблему", которая при правильно построенной системе шифрования не может быть решена с приемлемыми временными затратами.

Система открытого шифрования, предложенная в [1], отличается от рассмотренной, вместе с тем задача ее дешифрования для случая использования кода $\mathbf{K}$ над основным полем $\mathbf{F}_q$ также сводится к решению задачи определения по матрице $\mathfrak{B}$ матриц H и $\mathfrak{A}$. Если используется код из подполя $\mathbf{F}_q$ (альтернантный код), то задача определения матриц H и $\mathfrak{A}$ становится сложнее, но, по мнению авторов, она также решается методами, близкими к излагаемым ниже.

Основным результатом настоящей работы является построение алгоритма, который позволяет со сложностью $O(s^4 + sN)$ (измеряемой числом операций в поле $\mathbf{F}_q$, требуемых для его реализации) найти, зная матрицу $\mathfrak{B}$, матрицы H и $\mathfrak{A}$. В связи с этим отметим работу [4], в которой утверждается, что рассматриваемая система "открытого шифрования" имеет достаточно высокую стойкость к нападению.

§ 2. Алгоритм решения уравнения $\mathfrak{B} = H \cdot \mathfrak{A}$

Итак, перед нами стоит задача: по заданной матрице $\mathfrak{B}$ найти невырожденную матрицу H и элементы $x_1, \ldots, x_N \in \mathbf{F}$ и $z_1, \ldots, z_N \in \mathbf{F}_q \setminus \{0\}$, такие, что

$$\mathfrak{B} = H \cdot \mathfrak{A}(x_1, \ldots, x_N;\ z_1, \ldots, z_N). \tag{3}$$

Задачу будем решать в два этапа: сначала найдем числа $x_1, \ldots, x_N$, а затем числа $z_1, \ldots, z_N$ и матрицу H.

Прежде чем искать числа $x_1, \ldots, x_N$, сделаем несколько замечаний. Пусть $(H, x_1, \ldots, x_N, z_1, \ldots, z_N)$ – некоторое решение уравнения (3). Зафиксируем какие-нибудь $a, b \in \mathbf{F}_q$, $a \neq 0$, и найдем такие $h_{ij} \in \mathbf{F}_q$, $0 \leqslant i, j \leqslant s$, что $(ax + b)^i = \sum_{j=0}^{s} h_{ij} x^j$. Положим $H_1 = \| h_{ij} \|$; $d_i = 1$, если $x_i \neq \infty$, и $d_i = a^{-s}$, если $x_i = \infty$. Непосредственная проверка показывает, что

$$H_1 \cdot \mathfrak{A}(x_1, \ldots, x_N;\ d_1 z_1, \ldots, d_N z_N) = \mathfrak{A}(ax_1 + b, \ldots, ax_N + b;\ z_1, \ldots, z_N);$$

кроме того, матрица H_1 треугольная и поэтому невырожденная. Теперь из равенства

$$H \cdot H_1^{-1} \cdot \mathfrak{A}(ax_1 + b, \ldots, ax_N + b;\ d_1^{-1} z_1, \ldots, d_N^{-1} z_N) =$$
$$= H \cdot \mathfrak{A}(x_1, \ldots, x_N;\ z_1, \ldots, z_N) = \mathfrak{B}$$

видно, что $(H \cdot H_1^{-1},\ ax_1 + b, \ldots, ax_N + b;\ d_1^{-1} z_1, \ldots, d_N^{-1} z_N)$ также является решением уравнения (3). Аналогично, если

$$H_2 = \begin{bmatrix} 0 & 0 & \dots & 1 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 1 & \dots & 0 \\ 1 & 0 & \dots & 0 \end{bmatrix};$$

$d_i = x_i^{-s}$, если $x_i \neq 0, \infty$, и $d_i = 1$ в противном случае, то $H_2 \cdot \mathfrak{A}(x_1, \dots, x_N; d_1 z_1, \dots$ $\dots, d_N z_N) = \mathfrak{A}(1/x_1, \dots, 1/x_N;\ z_1, \dots, z_N)$. Значит, $(H \cdot H_2^{-1}, x_1^{-1}, \dots, x_N^{-1};\ d_1^{-1} z_1, \dots$ $\dots, d_N^{-1} z_N)$ – тоже решение уравнения (3). Как известно, любое дробно-линейное преобразование

$$\phi\colon\ x \to \frac{ax+b}{cx+d}, \qquad ad - bc \neq 0,$$

с коэффициентами из поля $\mathbf{F}_q$ представляется в виде композиции преобразований вида $x \to ax + b$ и $x \to 1/x$. С учетом этого получаем: для любого дробно-линейного преобразования ϕ существуют такие $z'_1, \dots, z'_N$ и матрица H_ϕ, что $(H \cdot H_\phi^{-1}, \phi(x_1), \dots$ $\dots, \phi(x_N);\ z'_1, \dots, z'_N)$ является решением уравнения (3), если $(H, x_1, \dots, x_N;$ $z_1, \dots, z_N)$ – решение уравнения (3).

Для любых трех различных чисел $x_1, x_2, x_3 \in \mathbf{F}_q \cup \{\infty\}$ можно подобрать такое дробно-линейное преобразование ϕ, что $\phi(x_1) = 1$, $\phi(x_2) = 0$, $\phi(x_3) = \infty$. Значит, существуют такие $x_4, \dots, x_N \in \mathbf{F}_q \setminus \{0,1\}$, $z'_1, \dots, z'_N \in \mathbf{F}_q \setminus \{0\}$ и матрица H, что $(H, 1, 0, \infty, x_4, \dots, x_N;\ z'_1, \dots, z'_N)$ – решение уравнения (3). Поскольку нам достаточно найти какое-нибудь решение, будем искать его именно в таком виде, т.е. положим $x_1 = 1$, $x_2 = 0$, $x_3 = \infty$.

Уравнение (3) представим в виде

$$\mathfrak{B} = H \cdot \mathfrak{A}_1(x_1, \dots, x_N) \cdot D = \| b_{ij} \|,$$

где $H = \| h_{ij} \|$, $\mathfrak{A}_1(x_1, \dots, x_N) = \mathfrak{A}(x_1, \dots, x_N;\ 1, \dots, 1)$ и $D = \operatorname{diag}(z_1, \dots, z_N)$, так что

$$H \cdot \mathfrak{A}(x_1, \dots, x_N) = \| a_{ij} \|, \quad a_{ij} = f_i(x_j), \quad f_i(x) = \sum_{j=0}^{s} h_{ij} x^j,$$

и, следовательно,

$$b_{ij} = z_j f_i(x_j)$$

(для любого $f \in \mathbf{F}_q[x]$, $\deg f \leqslant s$, положим $f(\infty)$ равным коэффициенту при x^s). Другими словами, в матрице D сосредоточены неизвестные z.

Найдем такие $c_{1i} \in \mathbf{F}_q$, $0 \leqslant i \leqslant s$, не все равные нулю, что для $j = 1, s+2, \dots$ $\dots, 2s$ выполняются равенства

$$\sum_{i=0}^{s} c_{1i} b_{ij} = 0.$$

Для этого необходимо решить систему из s однородных линейных уравнений от $s+1$ неизвестных. Эта система, очевидно, всегда имеет решение. Положим

$$F_1(x) = \sum_{i=0}^{s} c_{1i} f_i(x), \quad \beta_{1j} = \sum_{i=0}^{s} c_{1i} b_{ij}, \quad 1 \leqslant j \leqslant N.$$

Следовательно,

$$\beta_{1j} = \sum_{i=0}^{s} c_{1i} z_j f_i(x_j) = z_j F_1(x_j)$$

и, поскольку все числа z_j отличны от нуля, то из построения многочлена $F_1(x)$ вытекает, что $x_1, x_{s+2}, \ldots, x_{2s}$ являются его корнями. Заметим, что ни один из элементов $x_1, x_{s+2}, \ldots, x_{2s}$ не равен ∞, так как $x_3 = \infty$. Кроме того, $\deg f_i \leqslant s$, поэтому $\deg F_1 \leqslant s$. Значит, $F_1(x) = a_1(x - x_1)(x - x_{s+2}) \ldots (x - x_{2s})$. Из этого, в частности, следует, что при $j \neq 1, s+2, \ldots, 2s$ $F_1(x_j) \neq 0$ и $\beta_{1j} = z_j F_1(x_j) \neq 0$, а $\beta_{13} = z_3 F_1(x_3) = z_3 F_1(\infty) = a_1 z_3$.

Теперь найдем такие $c_{2i} \in \mathbf{F}_q$, $0 \leqslant i \leqslant s$, для которых выполняются равенства $\sum\limits_{i=0}^{s} c_{2i} b_{ij} = 0$ при $j = 2, s+2, \ldots, 2s$. Положим

$$F_2(x) = \sum_{i=0}^{s} c_{2i} f_i(x), \qquad \beta_{2j} = \sum_{i=0}^{s} c_{2i} b_{ij}.$$

Тогда

$$\beta_{2j} = z_j F_2(x_j) \quad \text{и} \quad F_2(x) = a_2(x - x_2)\cdot(x - x_{s+2}) \ldots (x - x_{2s}).$$

Поскольку $\beta_{2j} \neq 0$ при $3 \leqslant j \leqslant s+1$ и при $j \geqslant 2s+1$, то для этих значений j можно вычислить $b_j = \beta_{1j}/\beta_{2j}$. Но $b_j = z_j F_1(x_j)/z_j F_2(x_j) = a_1(x_j - x_1)(x_j - x_{s+2}) \ldots (x_j - x_{2s})/a_2 \cdot$ $\cdot (x_j - x_2)(x_j - x_{s+2}) \ldots (x_j - x_{2s}) = a_1(x_j - x_1)/a_2(x_j - x_2)$, $b_3 = \beta_{13}/\beta_{23} = a_1 z_3/a_2 z_3 =$ $= a_1/a_2$ и, собирая эти два равенства вместе, получаем: $b_j = b_3(x_j - x_1)/(x_j - x_2)$, откуда $x_j = (b_3 x_1 - b_j x_2)/(b_3 - b_j)$. С учетом того, что $x_1 = 1$ и $x_2 = 0$, для $j =$ $= 4, \ldots, s+1,\ 2s+1, \ldots, N$ окончательно имеем: $x_j = b_3/(b_3 - b_j)$.

Теперь найдем такие c_{3i}, $c_{4i} \in \mathbf{F}_q$, $0 \leqslant i \leqslant s$, что для $j = 1, 3, \ldots, s+1$ и для $j = 2, 3, \ldots, s+1$ выполняются равенства

$$\sum_{i=0}^{s} c_{3i} b_{ij} = 0 \quad \text{и} \quad \sum_{i=0}^{s} c_{4i} b_{ij} = 0$$

соответственно. Положим

$$F_3(x) = \sum_{i=0}^{s} c_{3i} f_i(x), \quad F_4(x) = \sum_{i=0}^{s} c_{4i} f_i(x),$$

$$\beta_{3j} = \sum_{i=0}^{s} c_{3i} b_{ij}, \qquad \beta_{4j} = \sum_{i=0}^{s} c_{4i} b_{ij}, \qquad 1 \leqslant j \leqslant N.$$

Из равенства $F_3(x_3) = F_3(\infty) = 0$ следует, что коэффициент при x^s в F_3 равен нулю, т.е. $\deg F_3 \leqslant s - 1$. Учитывая, что $F_3(x_1) = F_3(x_4) = \ldots = F_3(x_{s+1}) = 0$, получаем:

$$F_3(x) = a_3(x - x_1)(x - x_4) \ldots (x - x_{s+1}).$$

Аналогично $F_4(x) = a_4(x - x_2)(x - x_4) \ldots (x - x_{s+1})$. Тогда при $j \geqslant s+2$ будем иметь:

$$\beta_{3j}/\beta_{4j} = z_j F_3(x_j)/z_j F_4(x_j) = a_3(x_j - x_1)(x_j - x_4) \ldots (x_j - x_{s+1})/a_4(x_j - x_2) \cdot$$
$$\cdot (x_j - x_4) \ldots (x_j - x_{s+1}) = a_3(x_j - x_1)/a_4(x_j - x_2).$$

В частности, для $j = N$ получаем:

$$\beta_{3N}/\beta_{4N} = a_3(x_N - x_1)/a_4(x_N - x_2) = a_3 b_N/a_4 b_3,$$

откуда

$$a_3/a_4 = b_3 \beta_{3N}/b_N \beta_{4N} \quad \text{и} \quad \beta_{3j}/\beta_{4j} = b_3 \beta_{3N}/b_N \beta_{4N}(x_j - x_1)/(x_j - x_2).$$

Положим при $j = s+2, \ldots, 2s$ $b_j = \beta_{4N}/\beta_{3N} \cdot \beta_{3j}/\beta_{4j} \cdot b_N$. Тогда при этих значениях j выполняется равенство $b_j = b_3(x_j - x_1)/(x_j - x_2)$, как и для остальных значений j, значит, $x_j = b_3/(b_3 - b_j)$.

Еще раз опишем вкратце действия, необходимые для нахождения чисел x_j

1. Найти c_{1i}, $c_{2i} \in \mathbf{F}_q$, $0 \leqslant i \leqslant s$, такие что для $j = 1, s+2, \ldots, 2s$ и для $j = 2, s+2, \ldots, 2s$ выполняются равенства

$$\sum_{i=0}^{s} c_{1i} b_{ij} = 0 \quad \text{и} \quad \sum_{i=0}^{s} c_{2i} b_{ij} = 0$$

соответственно ($O(s^3)$ операций в поле $\mathbf{F}_q$).

2. Для $j = 3, \ldots, s+1, 2s+1, \ldots, N$ вычислить $\beta_{1j} = \sum_{i=0}^{s} c_{1i} b_{ij}$ и $\beta_{2j} = \sum_{i=0}^{s} c_{2i} b_{ij}$ и найти $b_j = \beta_{1j}/\beta_{2j}$ ($O(sN)$ операций).

3. Найти $c_{3i}, c_{4i} \in \mathbf{F}_q$, $0 \leqslant i \leqslant s$, такие что для $j = 1, 3, \ldots, s+1$ и для $j = 2, 3, \ldots, s+1$ выполняются равенства $\sum_{i=0}^{s} c_{3i} b_{ij} = 0$ и $\sum_{i=0}^{s} c_{4i} b_{ij} = 0$ соответственно ($O(s^3)$ операций).

4. Для $j = s+2, \ldots, 2s, N$ вычислить $\beta_{3j} = \sum_{i=0}^{s} c_{3i} b_{ij}$ и $\beta_{4j} = \sum_{i=0}^{s} c_{4i} b_{ij}$ и для $j = s+2, \ldots, 2s$ найти $b_j = (b_N \beta_{4N}/\beta_{3N})\beta_{3j}/\beta_{4j}$, где b_N найдено в пункте 2 ($O(s^2)$ операций).

5. Положить $x_1 = 1$, $x_2 = 0$, $x_3 = \infty$, $x_j = b_3/(b_3 - b_j)$ при $4 \leqslant j \leqslant N$ ($O(N)$ операций).

6. Для удобства дальнейших вычислений можно выбрать какое-нибудь $a \in \mathbf{F}_q$, отличное от всех x_j, $1 \leqslant j \leqslant N$, и заменить каждое x_j на $1/(a - x_j)$ ($O(N)$ операций). Полученный набор x_j по-прежнему будем элементом некоторого решения уравнения (3), однако, в нем не присутствует $x_j = \infty$.

Теперь приступим к нахождению чисел z_j и матрицы H. Заметим, что если каждый элемент матрицы D умножить на $a \in \mathbf{F}_q$, а каждый элемент H – на a^{-1}, то произведение $H \cdot \mathfrak{A} \cdot D$ останется неизменным. В связи с этим можно считать, что $z_1 = 1$.

Найдем такие $c_1, \ldots, c_{s+2} \in \mathbf{F}_q$, не все равные нулю, для которых выполнены равенства

$$\sum_{j=1}^{s+2} c_j b_{ij} = 0, \qquad 0 \leqslant i \leqslant s. \tag{4}$$

Для этого надо решить систему из $s+1$ однородных линейных уравнений с $s+2$ неизвестными. Заметим, что все числа c_j отличны от нуля, ибо в противном случае в матрице $\mathfrak{B}$ нашлись бы $s+1$ линейно зависимых столбцов. Поскольку $b_{ij} = z_j f_i(x_j)$, то равенства (4) могут быть записаны в виде

$$\sum_{j=1}^{s+2} c_j z_j f_i(x_j) = 0, \quad 0 \leqslant i \leqslant s,$$

или в матричной форме,

$$AC\bar{z} = 0,$$

где $A = \| a_{ij} \|$, $a_{ij} = f_i(x_j)$, $0 \leqslant i \leqslant s$, $1 \leqslant j \leqslant s+2$, $C = \mathrm{diag}(c_1, \ldots, c_{s+2})$, $\bar{z}$ – вектор-столбец $(z_1, \ldots, z_{s+2})^T$. Однако, как нетрудно заметить, $A = H \cdot \mathfrak{A}_1(x_1, \ldots, x_{s+2})$, откуда $H \cdot \mathfrak{A}_1(x_1, \ldots, x_{s+2}) \cdot C\bar{z} = 0$. Умножая слева последнее равенство на H^{-1}, получим $\mathfrak{A}_1(x_1, \ldots, x_{s+2}) C\bar{z} = 0$. Следовательно, числа z_j удовлетворяют соотношениям $\sum_{j=1}^{s+2} c_j z_j x_j^i = 0$, $0 \leqslant i \leqslant s$. С учетом того, что числа c_j и x_j уже известны, а $z_1 = 1$, получили линейную систему из $s+1$ уравнения с $s+1$ неизвестными $z_2, \ldots, z_{s+2}$, которая имеет единственное решение, поскольку определитель ее матрицы коэффициентов, равный $c_2 \ldots c_{s+2} \det \mathfrak{A}_1(x_2, \ldots, x_{s+2})$, отличен от 0. Решая эту систему, найдем элементы $z_1, \ldots, z_{s+2}$.

Если $H = \| h_{ik} \|$, $0 \leqslant i, k \leqslant s$, то

$$b_{ij} = z_j \sum_{k=0}^{s} h_{ik} x_j^k .$$

Зафиксировав какое-либо $i, 0 \leqslant i \leqslant s$, и изменяя j от 1 до $s+1$, получим систему линейных уравнений от $h_{i0}, \ldots, h_{is}$

$$\sum_{k=0}^{s} h_{ik} x_j^k = z_j^{-1} b_{ij}, \qquad 1 \leqslant j \leqslant s+1 .$$

Определитель матрицы этой системы есть определитель Вандермонда, поэтому числа $h_{i0}, \ldots, h_{is}$ находятся однозначно. Решив такую систему для каждого i, $0 \leqslant i \leqslant s$, мы определяем матрицу H.

Умножая обе части равенства (3) слева на H^{-1}, получаем

$$\mathfrak{A}(x_1, \ldots, x_N;\ z_1, \ldots, z_N) = H^{-1} \cdot \mathfrak{B} .$$

Поскольку первая строка матрицы $\mathfrak{A}(x_1, \ldots, x_N;\ z_1, \ldots, z_N)$ равна $(z_1, \ldots, z_N)$, то оставшиеся не найденными элементы z_j определяются соотношениями

$$z_j = \sum_{i=0}^{s} h'_{0i} b_{ij}, \quad s+3 \leqslant j \leqslant N, \quad \text{где} \quad H^{-1} = \| h'_{ij} \| .$$

Заметим, что для нахождения h'_{0i} нет необходимости вычислять всю матрицу H^{-1}, достаточно решить систему линейных уравнений $\sum_{i=0}^{s} h'_{0i} h_{i0} = 1$, $\sum_{i=0}^{s} h'_{0i} h_{ij} = 0$, $1 \leqslant j \leqslant s$. Однако матрица H^{-1} потребуется для декодирования, поэтому есть смысл вычислить ее сразу.

Еще раз коротко опишем алгоритм нахождения матриц H и $D = \mathrm{diag}(z_1, \ldots, z_N)$ и подсчитаем число операций, необходимых для его реализации, полагая при этом, что для решения системы из $s+1$ линейных уравнений над полем $\mathbf{F}_q$ требуется $O(s^3)$ операций.

1. Найти $c_1, \ldots, c_{s+2} \in \mathbf{F}_q$, такие что $\sum_{j=1}^{s+2} c_j b_{ij} = 0$, $0 \leqslant i \leqslant s$ ($O(s^3)$ операций).

2. Положить $z_1 = 1$ и найти $z_2, \ldots, z_{s+2} \in \mathbf{F}_q$, такие что $\sum_{j=1}^{s+2} c_j z_j x_j^i = 0$, $0 \leqslant i \leqslant s$ ($O(s^3)$ операций).

3. Для каждого $i, 0 \leqslant i \leqslant s$, найти $h_{i0}, \ldots, h_{is} \in \mathbf{F}_q$, такие что $\sum_{k=0}^{s} h_{ik} x_j^k = z_j^{-1} b_{ij}$, $1 \leqslant j \leqslant s+1$, и положить $H = \| h_{ij} \|$ ($O(s^4)$ операций).

4. Найти матрицу $H^{-1} = \| h'_{ij} \|$ и вычислить $z_j = \sum\limits_{i=0}^{s} h'_{0i} b_{ij}$, $s + 3 \leqslant j \leqslant N$ ($O(s^4 + sN)$ операций).

Общее число операций в поле $\mathbf{F}_q$, требующихся для решения уравнения (3) с помощью рассмотренного алгоритма, есть $O(s^4 + sN)$.

СПИСОК ЛИТЕРАТУРЫ

1. McEliece R.J. A Public–Key Creptosystem Based on Algebraic Coding Theory // DSN Progress Report 42:44. – Pasadena: Jet Propulsion Lab. CA, January–February, 1978. – P. 114–116.
2. Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory. Probl. Control and Inform. Theory. – 1986. – V. 15. – P. 19–34.
3. Мак-Вильямс Ф.Д., Слоэн Н.Дж. Теория кодов, исправляющих ошибки. – М.:Связь, 1979.
4. Security audit & Control Review. – ACM Press. – 1991. – V. 9, № 2. – P. 1–4.

Статья поступила 03.03.92