Открытые системы шифрования на основе кодов, корректирующих ошибки, и как некоторые из них можно расколоть

В. М. Сидельников

Основная цель данной работы рассказать со всеми подробностями о том, как можно расколоть за полиномиальное время систему открытого шифрования Нидеррайтера, построенную на основе кодов Рида-Соломона. Основные результаты этой статьи впервые изложены в работе Шестакова С.О и автора [2]. Как полагает автор, статья будет полезной молодым исследователям.

Не надо думать, что все системы открытого шифрования, основанные на кодах корректирующих ошибки, являются не стойкими. Данная работа является единственным известным примером кодовой системы открытого шифрования, которая раскалывается за полиномиальное время. Даже эту относительно простую систему расколоть, как будет видно ниже, весьма нетривиально. Для этого используются многие замечательные алгебраические конструкции: группы, матрицы, конечные поля и т.п. Как представляет себе автор, доказательство нестойкости даже отдельной системы шифрования, которая только деталями отличается от подобных стойких систем, имеет существенное как педагогическое, так и научное значение — не всё предлагаемое в открытой криптографии является качественным. Автор попытался сделать изложение замкнутым, но, по-видимому, это сделать ему полностью не удалось.

1. Несколько слов о теории кодов, корректирующих ошибки, и кодах Рида-Соломона

1.1. Основные понятия. В настоящем разделе будут даны только начальные сведения о теории кодирования, необходимые для определения систем открытого шифрования, предложенных Маклисом [1] и Нидеррайтером [4]. Для простоты, мы рассматриваем только частные случаи кодов, которые имеют наибольшее значение для криптографии. Значительно более полное изложение теории кодирования имеется в книгах [7] и [25].

Мы рассматриваем конечное поле $\mathbf{F}_q$, $q = p^l$, где p — простое число и l — положительное целое, содержащее q элементов. Множество $\mathbf{F}_q^n = \{\mathbf{x} = (x_1, \ldots, x_n) | x_j \in \mathbf{F}_q\}$, мы обычным образом рассматриваем как линейное пространство размерности n.

На пространстве $\mathbf{F}_q^n$ задана метрика Хемминга, которая определяется следующим образом. Расстояние $d(\mathbf{x}, \mathbf{y})$ между двумя векторами $\mathbf{x}$ и $\mathbf{y}$ из $\mathbf{F}_q^n$ равно числу координат, в которых эти векторы различаются. Например, расстояние между векторами $(0, 1, 2)$ и $(2, 1, 0)$ из $\mathbf{F}_3^3$ (трехмерное пространство над полем $\mathbf{F}_3 = \{0, 1, 2\}$ из трех элементов) равно 2, так как эти векторы различаются только в первой и последней координате. Метрическое пространстве $\mathbf{F}_q^n$ с метрикой Хемминга будем называть пространством Хемминга. На пространстве Хемминга рассматривают еще одну функцию $wt(\mathbf{x})$ — вес вектора $\mathbf{x}$, равный числу его ненулевых координат. Функции $d(\mathbf{x}, \mathbf{y})$ и $wt(\mathbf{x})$ связаны соотношениями $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$, $d(0, \mathbf{x}) = wt(\mathbf{x})$.

Кодом называется произвольное подмножество $\mathcal{K}$ пространства $\mathbf{F}_q^n$. Кодовое расстояние $d(\mathcal{K})$ кода $\mathcal{K}$ определяется как минимальное расстояние между двумя различными элементами $\mathcal{K}$, т.е. $d(\mathcal{K}) = \min_{\mathbf{x},\mathbf{y} \in \mathcal{K}; \mathbf{x} \neq \mathbf{y}} d(\mathbf{x}, \mathbf{y})$. Всюду далее мы в качестве кодов $\mathcal{K}$ будем рассматривать только линейные подпространства L пространства $\mathbf{F}_q^n$. Размерность L всегда будем обозначать буквой k. Такие коды называются $q-$значными линейными кодами. Их параметры будем коротко записываются в виде $[n, k, d]_q$, где n — длина кода $\mathcal{K}$, k — его размерность и $d = d(\mathcal{K})$ — его кодовое расстояние. Число $r = n - k$ обычно называют избыточностью кода.

Следует заметить, что кодовое расстояние линейного кода может представлено и несколько иным во многих случаях более удобным способом. А именно, $d(\mathcal{K})$ = минимальному весу ненулевого элемента кода $\mathcal{K}$ (доказать самостоятельно).

Определенные выше коды используются для коррекции ошибок при передачи информации в канале связи. Схема такого использования состоит в следующем.

Под одиночной ошибкой типа замещения мы понимаем замену одного из символов в векторе $\mathbf{x} \in \mathbf{F}_q^n$ на другой символ. Если в векторе $\mathbf{x}$ произошло t ошибок, то t координат изменило свое значение. То, что пространство $\mathbf{F}_q^n$ является метрическим, позволяет утверждать, что $t-$кратная ошибка превращает кодовый вектор $\mathbf{x}$ в вектор $\mathbf{x}'$, отстоящий от $\mathbf{x}$ на расстояние t, т.е. $d(\mathbf{x}, \mathbf{x}') = t$. Таким образом, если в канале связи происходит не более, чем t ошибок, то искаженный кодовый вектор $\mathbf{x}'$ находится в шаре (в метрике Хемминга) радиуса t с центром в точке $\mathbf{x} \in \mathcal{K}$.

1.2. Геометрическая интерпретация кода. Если все шары радиуса t с центрами в кодовых точках кода $\mathcal{K}$ не пересекаются, то из очевидных геометрических соображений следует, что код может исправить любые t или меньше ошибок, которые поразили кодовый вектор $\mathbf{x}$ в канале связи. Для этого необходимо использовать процедуру декодирования, которая находит тот центр шара $\mathbf{x}$ (кодовый вектор), к которому принадлежит искаженный вектор $\mathbf{x}'$. Из сказанного выше вытекает, что если код имеет кодовое расстояние $d(\mathcal{K}) \geq 2t+1$, то он может корректировать все ошибки кратности $\leq t$.

Вектору $\vec{a} = (a_1, \ldots, a_k)$, $a_j \in \mathbf{F}_q$, который переносит информацию, поставим в соответствие кодовый вектор $\mathbf{x}(\vec{a}) \in \mathcal{K}$. Для передачи информационного вектора $\vec{a}$ по каналу связи с шумами в канал вместо $\vec{a}$ посылают кодовый вектор $\mathbf{x}(\vec{a})$. На выходе канала после декодирования определяется вектор $\mathbf{x}(\vec{a})$, а затем и информационный вектор $\vec{a}$.

Рассмотренную геометрическую модель коррекции ошибок можно построить из-за того, что $\mathbf{F}_q^n$ является метрическим пространством, метрика которого в согласована с видом искажений, которые возникают в канале связи. Можно сказать, что с геометрической точки зрения теория кодов, исправляющих ошибки, представляет собой науку, которая занимается упаковками шаров в метрических пространствах, в частности, в пространстве Хемминга, а также задачами декодирования кодов того или иного вида. Таким образом, такое весьма абстрактное математическое понятие, как метрическое пространство, оказывается весьма полезным для содержательных и наглядных представлений кодов $\mathcal{K}$, корректирующих ошибки, и в конечном итоге для их построения и использования.

Одной из основных задач теории кодирования является задача построения кода длины n с кодовым расстоянием d с возможно большим числом элементов, т.е. в случае линейного кода с возможно большой размерностью k. За многие годы развития теории кодирования создано большое число разнообразных кодов. Мы остановимся только на относительно узком классе: классических и давно известных кодах Рида-Соломона и кодах Боуза-Чоудхури-Хоквингема (БЧХ-код). Код Рида-Соломона является частным случаем БЧХ-кода.

1.3. Проверочная и порождающая матрицы линейного кода и их свойства. Будем пользоваться без объяснений стандартными понятиями теории конечных полей и линейной алгебры.

Подпространство $\mathcal{K}$ (линейный код над конечным полем $\mathbf{F}_q$) пространства $\mathbf{F}_q^n$ может быть определено (задано) двумя способами: как своим базисом так и базисом пространства $\mathcal{K}^\perp$, двойственного к $\mathcal{K}$ (определение ниже). Первый способ определения кодов является более естественным, но зато второй является во многих случаях более удобен для их построения и исследования их свойств. Он преимущественно используется в теории кодирования. Мы также часто будем пользоваться вторым способом задания линейного кода. Подробно объясним что это такое.

Скалярное произведение $\langle \mathbf{x}, \mathbf{y} \rangle$ векторов $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbf{F}_q^n$ в поле $\mathbf{F}_q$ определяется соотношением

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{j=1}^{n} x_j y_j, \tag{1}$$

где сложение и умножение в последней сумме выполняется в поле $\mathbf{F}_q$.

Код $\mathcal{K}^\perp$ над $\mathbf{F}_q$ состоит из всех векторов $\mathbf{b} \in \mathbf{F}_q^n$ таких, что $\langle \mathbf{b}, \mathbf{a} \rangle = 0$ для всех $\mathbf{a} \in \mathcal{K}$. По другому, если $\mathbf{a}_1, \ldots, \mathbf{a}_k$ — базис кода $\mathcal{K}$, то базисом кода $\mathcal{K}^\perp$ являются векторы $\mathbf{b}_1, \ldots, \mathbf{b}_{n-k}$, для которых $\langle \mathbf{b}_j, \mathbf{a}_s \rangle = 0$ для всех $s = 1, \ldots, k$. Отметим, что сумма размерностей кодов $\mathcal{K}$ и $\mathcal{K}^\perp$ равна n (доказать самостоятельно).

Матрица B, строками которой являются базисные векторы кода $\mathcal{K}^\perp$ (их число $n-k$) называется проверочной матрицей кода $\mathcal{K}$, а матрица A, строками которой являются базисные векторы кода $\mathcal{K}$,

называется порождающей матрицей кода $\mathcal{K}$. Таким образом, коду $\mathcal{K}$ принадлежат все векторы $\mathbf{a}$, для которых выполнено

$$B\mathbf{a}^T = 0, \quad \mathbf{a} \in \mathbf{F}_q^n, \tag{2}$$

где значок ^{T} о обозначает "транспонирование" соответствующего объекта (общепринятое обозначение), или все векторы $\mathbf{a}$, которые имеют вид

$$\mathbf{a} = \vec{d}A, \quad \vec{d} \in \mathbf{F}_q^k, \ \mathbf{a} \in \mathbf{F}_q^n. \tag{3}$$

Заметим, что в формуле (2) $\mathbf{a}^T$ — столбец высоты n. Матрицы B и A по определению взаимно ортогональны: $A \cdot B^T = 0$, $B \cdot A^T = 0$.

Утверждение 1. *Код $\mathcal{K}$ имеет кодовое расстояние d, если выполнены два условия*

i. *Любой комплект из $d-1$ столбцов матрицы B является линейно-независимым.*

ii. *Найдется комплект из d столбцов матрицы B, который является линейно-зависимым.*

Это достаточно простое утверждение может быть доказано самостоятельно. Отметим только, что если выполнено лишь условие i, то $d(\mathcal{K}) \geq d$.

С помощью утверждения 1 все или почти все методы построения кодов $\mathcal{K}$ с кодовым расстоянием d сводятся к построению проверочной матрицы B, у которой любой комплект из $d-1$ ее столбцов является линейно-независимым.

Наиболее известными матрицами B, для которых выполнено утверждение 1, является матрица

$$B = B_{\mathfrak{A}} = \begin{pmatrix} \alpha_1^0 & \alpha_2^0 & \cdots & \alpha_n^0 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{d-2} & \alpha_2^{d-2} & \cdots & \alpha_n^{d-2} \end{pmatrix}, \ d > 2, \tag{4}$$

где $n \leq q-1$ и $\mathfrak{A} = \{\alpha_1, \alpha_1, \ldots, \alpha_n\}$ — различные ненулевые элементы поля $\mathbf{F}_q$. Столбцы любого комплекта из $d-1$ столбцов матрицы B является линейно-независимыми. Это следует из того, что определитель

$$\begin{vmatrix} \beta_1^0 & \beta_2^0 & \cdots & \beta_{d-1}^0 \\ \beta_1 & \beta_2 & \cdots & \beta_{d-1} \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_{d-1}^2 \\ \vdots & \vdots & \cdots & \vdots \\ \beta_1^{d-2} & \beta_2^{d-2} & \cdots & \beta_{d-1}^{d-2} \end{vmatrix}, \ \beta_j \in \{\alpha_1, \alpha_2, \ldots, \alpha_n\}, \tag{5}$$

с попарно различными β_j является отличным от 0 определителем Вандермонда.

Множество $\mathfrak{A}$ часто расширяют, а именно, добавляют к нему элементы $0 \in \mathbf{F}_q$ и особый элемент ∞. Мы далее будем полагать, что матрица B в (4) определена именно для такого расширенного множества $\mathfrak{A}$. О подробностях такого определения удобно рассказать ниже в разделе 1.4.

Нумерацию столбцов матрицы B будем производить с помощью элементов множества $\mathfrak{A}$. Так столбец с номером α является $j-$ым столбцом, если $\alpha = \alpha_j$. Совершенно аналогично поступаем с координатами вектора $\mathbf{x} = (x_{\alpha_1}, x_{\alpha_2}, \ldots, x_{\alpha_n}) \in \mathbf{F}_q^n$, их также индексируем элементами множества $\mathfrak{A}$, которые записаны в определенном порядке.

1.4. Коды Рида-Соломона. Мы рассмотрим три вида кодов Рида-Соломона длин $n = q-1$, q, $q+1$. Все они имеют в качестве проверочной матрицу вида (4), но различные множества $\mathfrak{A}$.

Тип 1. $n = q-1$. В этом случае множество $\mathfrak{A}$ состоит из всех ненулевых элементов поля $\mathbf{F}_q$.

Тип 2. $n = q$. В этом случае множество $\mathfrak{A}$ состоит из всех элементов поля $\mathbf{F}_q$. Следует сказать, что столбец $(\alpha_j^0, \alpha_j, \ldots, \alpha_j^{d-2})^T$, у которого $\alpha_j = 0$ имеет вид $(1, 0, \ldots, 0)^T$.

Тип 3. $n = q+1$, $d > 3$. В этом случае множество $\mathfrak{A}$ состоит из всех элементов поля $\mathbf{F}_q$ и еще одного элемента ∞ (бесконечности). Предполагается, что элемент ∞ обладает естественными свойствами этого понятия. Например, $a\infty = \infty$, $a \neq 0$, $\frac{a}{\infty} = 0$ и т.п. Столбец $(\alpha_j^0, \alpha_j, \ldots, \alpha_j^{d-2})^T$, у которого $\alpha_j = \infty$ по определению имеет вид $(0, 0, \ldots, 1)^T$. Более общо, мы считаем, что значение многочлена $f(x) = \sum_{s=0}^{d-2} f_s x^s$ степени не выше $d-2$ в точке ∞ является коэффициент f_{d-2}. В частности, $f(\infty) = 0$, если степень $f(x)$ меньше $d-2$. В этом случае мы говорим, что $f(x)$ имеет корень ∞. Можно сказать, что мы рассматриваем проективное пространство $\mathbf{F}_q \cup \{\infty\}$ и многочлены на нем.

Коды Рида-Соломона всех типов будем обозначать одним символом $RS_q(n,d)$. Все они имеют параметры $[n, n-d+1, d]_q$ и являются, так называемым, $q-$значными МДР-кодами (см. [7]), а именно кодами, которые имеют максимально возможную размерность $n-d+1$ при заданных n и d.

Одна из модификаций кода типа 3 (длины $n = q+1$) будет далее использована как основа для построения "системы открытого шифрования", которую мы будем подробно изучать. В частности, мы рассмотрим группу автоморфизмов (определение — ниже) этого кода. Эта группа имеет наиболее сложное строение по сравнению с группами автоморфизмов кодов типов 1. и 2. Поэтому мы сначала достаточно подробно изучим группу автоморфизмов кодов типа 2., а затем в основном без доказательства приведем нужные свойства группы автоморфизмов кода типа 3.

Надо сказать, что коды типа 3., в некотором смысле, являются наиболее интересным среди, определенных ранее трех типов кодов Рида-Соломона. В частности, они имеют наиболее мощную группу автоморфизмов и наибольшую длину и размерность при заданном кодовом расстоянии d. Коды типа 1. используются для построения циклических кодов Боуза-Чоудхури-Хоквингема. Коды $RS_q(n,d)$ всех типов могут быть заданы (определены) и несколькими другими способами.

1.5. Код Боуза-Чоудхури-Хоквингема. Предположим, что поле $\mathbf{F}_r, r = p^{l'}$, где число l' делит l $(l'|l)$, является подполем поля $\mathbf{F}_q$, $q = p^l$. В этом случае мы будем рассматривать $r-$значным подкод кода $RS_q(n,d)$, $n = q-1$, который состоит из всех векторов $RS_q(n,d)$, координаты которых принадлежат полю $\mathbf{F}_r$. Этот код называют кодом Боуза-Чоудхури-Хоквингема (обозначение: $BCH_r(n,d)$). Он имеет параметры $[q-1, d', k']_r$, где $d' \geq d$, $k' \geq q-1-(d-1-[\frac{d-1}{r}])\frac{l}{l'}$. По поводу этих оценок и замечательных свойств кода $BCH_r(n,d)$ см. книгу [7].

Следует обратить внимание на то, что размерности кода $RS_q(n,d)$ и кода $BCH_r(n,d)$ вычисляются над разными полями: размерность первого — над $\mathbf{F}_q$, а размерность второго — над его подполем $\mathbf{F}_r$.

1.6. Группа автоморфизмов кода $RS_q(n,d)$, $n = q$. Если переставить координаты кодового вектора $\mathbf{a}$ кода $\mathcal{K}$, то полученный вектор $\mathbf{a}'$ может как принадлежать так и не принадлежать коду $\mathcal{K}$. Если перестановка координат σ такова, что $\sigma(\mathbf{a}) = \mathbf{a}' \in \mathcal{K}$ для всех $\mathbf{a} \in \mathcal{K}$, то она называется автоморфизмом кода $\mathcal{K}$. Очевидно, что если σ' — другой автоморфизм, то произведение $\sigma \cdot \sigma'$ также является автоморфизмом. Поэтому все автоморфизмы кода $\mathcal{K}$ образуют группу $\Sigma_{\mathcal{K}}$, которая называется группой автоморфизмов кода $\mathcal{K}$. Заметим, что на множестве перестановок координат векторов пространства $\mathbf{F}_q^n$ можно естественным образом определить операцию $\cdot$, по отношению к которой все они образуют группу S_n порядка $n!$, называемую симметрической группой.

Перестановку σ удобно представлять себе в виде перестановочной матрицы $\Gamma_\sigma = \Gamma = \|\gamma_{i,j}\|$, которая реализует эту перестановку в виде матричного умножения. А именно, элемент матрицы $\gamma_{i,j}$ равен 1 тогда и только тогда, когда координата с номером i переходит посредством действия σ в координату с номером j. Во всех остальных случаях $\gamma_{i,j} = 0$. Таким образом, матрица Γ представляет из себя матрицу, у которой в любой строке и в любом столбце имеется ровно одна 1. Перестановочная матрица Γ реализует перестановку σ координат вектора $\mathbf{a}$ в виде матричного умножения следующим образом $\sigma(\mathbf{a}) = \mathbf{a}\Gamma$. Матричная группа автоморфизмов $G = G_{\mathcal{K}}$ образована всеми матрицами Γ_σ, у которых $\sigma \in \Sigma_{\mathcal{K}}$.

Если $\Gamma \in G_{\mathcal{K}}$, а матрица B является проверочная матрица кода $\mathcal{K}$, то $B \cdot \Gamma$, очевидно, также является проверочной матрицей этого кода $\mathcal{K}$. Поэтому она может быть представлена в виде $B \cdot \Gamma = h \cdot B$, где невырожденная матрица h размера $n-k \times n-k$ является матрицей перехода от одного базиса пространства строк матрицы B к другому B'. Последнее высказывание на языке матриц записывается как раз в виде $B' = h \cdot B$.

Интересно отметить, что указанное отображение $\Gamma \to h$ реализует гомоморфизм матричной группы $G_{\mathcal{K}}$ автоморфизмов кода $\mathcal{K}$ (матрицы размера $n \times n$) в матричную группу, образованную матрицами h размера $n-k \times n-k$. Ядро $J(\mathcal{K})$ этого гомоморфизма образуют элементы Γ, которые оставляют на месте все векторы кода $\mathcal{K}$. Поэтому матрицы h, на которые отображается группа $G_{\mathcal{K}}$ посредством соответствия $B \cdot \Gamma = h \cdot B$, изоморфна факторгруппе $G_{\mathcal{K}}/J(\mathcal{K})$. Так как далее мы ограничимся рассмотрением только кодов, у которых ядро $J(\mathcal{K})$ тривиально (состоит из одного элемента), то мы всегда будем полагать, группа образованная матрицами h изоморфна группе $G_{\mathcal{K}}$. К таким кодам относятся коды $RS_q(n,d)$ и коды $BCH_q(n,d)$. Доказательство этого утверждения в более общей форме см. ниже (Лемма 2).

Рассмотрим ансамбль (множество) $\mathcal{B}_{\mathcal{K}}$ кодов, определяемых проверочными матрицами из множества $\mathfrak{B} = \{B \cdot \Gamma | \Gamma \in S_n\}$, где B — одна, не важно какая, матрица вида (4). Число $\mathcal{Ч}_q(n,d)$ различных

(как множеств) кодов $\mathcal{K} = RS_q(n,d)$ в ансамбле $\mathcal{B}_\mathcal{K}$ (по другому, кодов с проверочной матрицей вида (4)), как нетрудно видеть, равно

$$\text{Ч}_q(n,d) = \frac{n!}{|G_\mathcal{K}|}, \tag{6}$$

где $\mathcal{K} = RS_q(n,d)$ — один из фиксированных кодов Рида-Соломона с проверочной матрицей (4).

Как мы видим, число различных кодов Рида-Соломона полностью определяется порядком его группы автоморфизмов. К настоящему времени группа автоморфизмов $G_\mathcal{K}$ кода $\mathcal{K} = RS_q(n,d)$ не вычислена. Можно только утверждать, в $G_{RS_q(n,d)}$ входят подстановочные матрицы, которые реализуют подстановку $x \to ax, a \in \mathbf{F}_q \setminus \{0\} = \mathbf{F}_q^*$, элементов поля $\mathbf{F}_q$ в себя. Эти матрицы образуют группу, которая изоморфна, так называемой, мультипликативной группе поля $\mathbf{F}_q$. Эта группа является циклической, поэтому и коды Рида-Соломона также как и коды Боуза-Чоудхури-Хоквингема с помощью соответствующей нумерации множества $\mathfrak{A}$ могут быть сделаны циклическими. На этом здесь останавливаться не будем (см. [7]).

1.7. Число проверочных матриц кода $RS_q(n,d)$. Если h — невырожденная матрица размера $d-1 \times d-1$, то, как нетрудно видеть, проверочные матрицы B и hB определяют один и тот же код $RS_q(n,d)$. В качестве задачи для самостоятельного доказательства приведем следующее утверждение. *Матрицы B и hB различны, если $h \neq E$ (единичная матрица).* Отсюда следует, что число различных проверочных матриц, которые определяют один и тот же код $RS_q(n,d)$, равно $N_{q,d-1}$, где $N_{q,s}$ — число невырожденных квадратных матриц h размера $s \times s$.

Лемма 1. *Число $N_{q,s}$ равно*

$$N_{q,s} = (q^s-1)(q^s-q)\cdots(q^s-q^{s-1}). \tag{7}$$

Доказательство. Первую строку невырожденной матрицы h над полем $\mathbf{F}_q$ размера $s \times s$ можно выбрать q^s-1 способами — все векторы длины s, исключая нулевой. Вторую строку — q^s-q способами — все векторы, которые не пропорциональны первой строке. Третью строку — q^s-q^2 способами — все векторы, которые не входят в подпространство размерности 2 пространства $\mathbf{F}_q^s$, натянутое на первые две строки. И так далее. Наконец, последнюю строку h можно выбрать q^s-q^{s-1} способами — все векторы которые не принадлежат $s-1$−мерному пространству натянутому на первые $s-1$ строк h. Отсюда вытекает лемма 1.

Заметим, что вычислить число различных матриц достаточно просто; вместе с тем вычислить число различных кодов $RS_q(n,d)$ значительно сложнее.

1.8. Обобщенные коды $RS_q(n,d)$, $n = q+1$ Рида-Соломона. Нам удобно рассмотреть несколько более широкий по сравнению с $RS_q(n,d)$ класс кодов, который мы будем называть обобщенные коды Рида-Соломона и обозначать их тем же символом $RS_q(n,d)$.

Пусть $\mathbf{F}'_q = \mathbf{F}_q \cup \infty$ — поле, к которому добавлен элемент ∞. Рассмотрим матрицу

$$C = \begin{pmatrix} z_1\alpha_1^0 & z_2\alpha_2^0 & \cdots & z_n\alpha_n^0 \\ z_1\alpha_1 & z_2\alpha_2 & \cdots & z_n\alpha_n \\ z_1\alpha_1^2 & z_2\alpha_2^2 & \cdots & z_n\alpha_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ z_1\alpha_1^{d-2} & z_2\alpha_2^{d-2} & \cdots & z_n\alpha_n^{d-2} \end{pmatrix}, \quad d > 3,\ n = q = 1, \tag{8}$$

где $\alpha_j \in \mathbf{F}'_q$, $\alpha_j \neq \alpha_i$ при $j \neq i$ и при $\alpha_j = \infty$ соответствующий столбец матрицы C имеет вид $(0,\ldots,0,z_j)^T$.

Также как для обычного код Рида-Соломона, обобщенный код длины $n = q+1$ имеет кодовое расстояние равное d и размерность $n-d+1$. Это доказывается почти точно также как и для обычного кода.

Матрица C, очевидно, может быть представлена в виде $C = B \cdot D$, где $D = \operatorname{diag}(z_1, z_2, \ldots, z_n)$, $z_j \in \mathbf{F}_q \setminus \{0\}$, — диагональная матрица и B — проверочная матрица кода Рида-Соломона типа 3. Преобразованная матрица C будет выступать далее как проверочная матрица системы открытого шифрования. В этой связи значительный интерес представляет строение группы обобщенных автоморфизмов кода Рида-Соломона с проверочной матрицей B, к изучению которой мы переходим.

Обобщенный код $BCH_r(n,d)$ определяется аналогично тому, как это было сделано в разделе 1.5: $BCH_r(n,d) = RS_q(n,d) \cap \mathbf{F}_r^n$, т.е. коду $BCH_r(n,d)$ принадлежат все векторы кода $RS_q(n,d)$, координаты которых принадлежат подполю $\mathbf{F}_r$ поля $\mathbf{F}_q$. Обобщенные коды $BCH_r(n,d)$ включают в себя и, так называемые, кода Гоппы (см. [7]).

Код можно задать и с помощью своей проверочной матрицы над полем $\mathbf{F}_r$ размера $n-k \times n$, где k — размерность (над $\mathbf{F}_r$) кода $BCH_r(n,d)$. Эта матрица также может иметь вид (8). Определить размерность k даже в частных случаях обобщенных кодов $BCH_r(n,d)$ в отличии от размерности любого кода $RS_q(n,d)$ очень нетривиально. В общем случае сделать это не представляется возможным.

1.9. Группа обобщенных автоморфизмов кода $RS_q(n,d)$, $n = q+1$, Рида-Соломона. . Если в качестве обычных автоморфизмов кода $\mathcal{K}$ выступали перестановочные матрицы Γ, то в качестве обобщенных автоморфизмов выступают матрицы вида $\Lambda = \Gamma \cdot D$, где D — невырожденная диагональная матрица, которые носят название унипотентных. Другими словами, Λ — перестановочная матрица, у которых ненулевыми элементами являются ненулевые элементы поля $\mathbf{F}_q$.

Унипотентные матрицы сохраняют расстояние Хемминга. А именно, $d(\mathbf{a},\mathbf{b}) = d(\mathbf{a}\Lambda, \mathbf{b}\Lambda)$. Как будет видно ниже, это свойство позволяет использовать эти матрицы в системе открытого шифрования. Нашей основной целью является получение нетривиальных нижних верхних оценок порядка группы обобщенных автоморфизмов кода $RS_q(n,d)$ и затем оценок для числа различных кодов $RS_q(n,d)$.

Теперь переформулируем для обобщенных автоморфизмов некоторые из определений раздела 1.6.

Если унипотентная матрица Λ такова, что $\mathbf{a}\Lambda = \mathbf{a}' \in \mathcal{K}$ для всех $\mathbf{a} \in \mathcal{K}$, то она называется обобщенным автоморфизмом кода $\mathcal{K}$. Очевидно, что если Λ' — другой автоморфизм, то произведение $\Lambda \cdot \Lambda'$ также является автоморфизмом. Поэтому все обобщенные автоморфизмы кода $\mathcal{K}$ образуют группу $\Xi_{\mathcal{K}}$, которая называется группой обобщенных автоморфизмов кода $\mathcal{K}$. Элементами группы $\Xi_{\mathcal{K}}$ являются, так называемые, унипотентные матрицы размера $n \times n$. Также как в разделе 1.6 можно рассмотреть представление $H_{\mathcal{K}}$ группы обобщенных автоморфизмов $\Xi_{\mathcal{K}}$ в виде невырожденных матриц над $\mathbf{F}_q$ размера $n-k \times n-k$. А именно, элементу Λ из $\Xi_{\mathcal{K}}$ сопоставим матрицу $h = h_\Lambda$, которая определяется соотношением

$$h_\Lambda \cdot B = B \cdot \Lambda. \tag{9}$$

Произведение $\Lambda \cdot \Lambda'$ двух элементов из $\Xi_{\mathcal{K}}$ соответствует произведение $g(\Lambda \cdot \Lambda') = h_{\Lambda'} \cdot h_\Lambda$ двух элементов из $H_{\mathcal{K}}$. Заметим, что порядок следования сомножителей в $H_{\mathcal{K}}$ обратный по сравнению с $\Xi_{\mathcal{K}}$. Поэтому рассматриваемое отображение является гомоморфизмом $g : \Lambda \to h_\Lambda$ группы $\Xi_{\mathcal{K}}$ в группу матриц размера $n-k \times n-k$ над полем $\mathbf{F}_q$.

Лемма 2. *Для кода $\mathcal{K} = RS_q(n,d)$ гомоморфизм g является изоморфизмом, т.е $|\Xi_{\mathcal{K}}| = |H_{\mathcal{K}}|$.*

Доказательство. Ядро гомоморфизма g тривиально. Это следует из-за того, что матрица B не содержит пропорциональных столбцов и поэтому $B \neq B \cdot \Lambda$ для любой неединичной унипотентной матрицы Λ. Поэтому среди неединичных унипотентных матриц Λ не существует такой, что $\mathbf{a} = \mathbf{a}\Lambda$ для всех $\mathbf{a} \in RS_q(n,d)$. Лемма доказана.

Теорема 1. *Порядок группы $\Xi_{\mathcal{K}}$ автоморфизмов кода Рида-Соломона $\mathcal{K} = RS_q(n,d)$ не превосходит $N_{q,d-1}$, где $N_{q,s}$ — число невырожденных квадратных матриц h размера $s \times s$ над полем $\mathbf{F}_q$.*

Доказательство. Как следует из леммы 2 $|\Xi_{\mathcal{K}}| = |H_{\mathcal{K}}|$. Поэтому $|\Xi_{\mathcal{K}}| \leq N_{q,n-k}$, $k = n-d+1$, ибо, очевидно, что $|H_{\mathcal{K}}|$ не превосходит числа всех матриц размера $d-1 \times d-1$ над полем $\mathbf{F}_q$. Теорема доказана.

Хотя оценка для числа $\Xi_{\mathcal{K}}$ во многих случаях, по-видимому, весьма грубая, ничего лучшего не известно.

Рассмотрим ансамбль (множество) $\mathcal{A}_{\mathcal{K}}$, $\mathcal{K} = RS_q(n,d)$, кодов, определяемых проверочными матрицами из множества $\mathfrak{B} = \{B\Lambda | \Lambda \in U_{q,n}\}$, где B — одна, не важно какая, матрица вида (4), а $U_{q,n}$ — множество всех унипотентных матриц над полем $\mathbf{F}_q$. Заметим, что ансамбль $\mathcal{A}_{\mathcal{K}}$ совпадает с множеством кодов, проверочные матрицы которых имеют вид (8). Кроме того, нетрудно установить, что $|U_{q,n}| = n!(q-1)^n$. Нас будет интересовать число различных кодов в ансамбле $\mathcal{A}_{\mathcal{K}}$.

По тем же соображениям, что приведены в разделе 1.6, для числа $A_q(n,d)$ различных обобщенных кодов Рида-Соломона $\mathcal{K} = RS_q(n,d)$ в ансамбле $\mathcal{A}_{\mathcal{K}}$ имеет место равенство

$$A_q(n,d) = \frac{n!(q-1)^n}{|\Xi_{\mathcal{K}}|}. \tag{10}$$

К сожалению, группа $\Xi_{\mathcal{K}}$ обобщенных автоморфизмов кода Рида-Соломона не известна. Поэтому мы не можем воспользоваться равенством (10) для вычисления числа $A_q(n,d)$.

Из теоремы 1 и соотношений (7) и (10) следует

Следствие 1. *Для числа $A_q(n,d)$ различных обобщенных Рида-Соломона $\mathcal{K} = RS_q(n,d)$ в ансамбле $\mathcal{A}_\mathcal{K}$ имеет место оценка*

$$A_q(n,d) \geq \frac{n!(q-1)^n}{N_{q,k}} = \frac{n!(q-1)^n}{(q^{d-1}-1)(q^{d-1}-q)\cdots(q^{d-1}-q^{d-2})}, \tag{11}$$

где $k = n-d+1$ — размерность кода $\mathcal{K} = RS_q(n,d)$ и $N_{q,k}$ — число различных невырожденных матриц размера $k \times k$.

Далее мы докажем, что группа $\Xi_\mathcal{K}$ содержит подгруппу, изоморфную группе дробно-линейных преобразований. Строение последней группы мы изучим в следующем разделе.

1.10. Группа дробно-линейных преобразований. Элементами группы дробно-линейных преобразований Φ_q множества $\mathbf{F}'_q = \mathbf{F}_q \cup \{\infty\}$ в себя являются дробно-линейные функции $\phi(x) = \frac{ax+b}{cx+e}$, отличные от постоянной, т.е. функции, у которых определитель матрицы $\begin{pmatrix} a & b \\ c & e \end{pmatrix}$ отличен от нуля. Очевидно, каждое дробно-линейных преобразование $\phi(x)$ взаимно однозначно отображает множество $\mathbf{F}'_q$ в себя.

Множество Φ_q действительно является некоммутативной группой. "Умножением" $\otimes$ в ней служит суперпозиция функций, т.е. $\phi \otimes \phi' = \phi(\phi'(x))$. Группа $\Phi_q = PGL(2,q)$ имеет порядок $(q+1)q(q-1)$. Очень интересным свойством группы Φ_q является ее трижды транзитивность. Это означает, что для любых двух пар троек (a_1,a_2,a_3) и (b_1,b_2,b_3), $a_i, b_i \in \mathbf{F}'_q$, с попарно различными координатами в группе Φ_q найдется элемент ϕ (всегда один), для которого выполнено $\phi(a_i) = b_i$, $i = 1,2,3$. Доказательство этих свойств несложно и предоставляется читателю (см. также [23] и [24]).

Теорема 2. *Группа $\Xi_\mathcal{K}$ обобщенных автоморфизмов кода $\mathcal{K} = RS_q(n,d)$, $n = q+1$, Рида-Соломона с проверочной матрицей B (см. (4)) содержит подгруппу, которая изоморфна группе дробно-линейных преобразований множества $\mathbf{F}'_q$.*

Доказательство. Как и выше, будем индексировать столбцы матрицы B (см. (4)) элементами множества $\mathbf{F}'_q$. Так столбец $B(\alpha_j) = (\alpha_j^0, \alpha_j^1, \ldots, \alpha_j^{d-2})^T$ имеет номер (индекс) α_j.

Пусть $\phi(x) = \frac{ax+b}{cx+e}$ — дробно-линейная функция. Через Γ_ϕ обозначим подстановочную матрицу, реализующую перестановку $x \to \phi(x)$ элементов множества $\mathbf{F}'_q$ и через $D_\phi =$
$\mathrm{diag}((c\alpha_1+e)^{d-2}, (c\alpha_2+e)^{d-2}, \ldots, (c\alpha_n+e)^{d-2})$ — диагональную матрицу, определяемую значениями знаменателя функции $\phi(x)$ на всех элементах множества $\mathbf{F}'_q$.

Прямое вычисление показывает, что $B(\alpha_j)\cdot\Gamma_\phi\cdot D_\phi = ((c\alpha_j+e)^{d-2}, (a\alpha_j+b)(c\alpha_2+e)^{d-3}, \ldots, (a\alpha_j+b)^{d-3}(c\alpha_2+e), (a\alpha_j+b)^{d-2})^T$. Каждый многочлен $(ax+b)^{d-2-i}(cx+e)^i$ может быть представлен как линейная функция мономов $1, x, , \ldots, x^{d-2}$. Поэтому столбец $B(\alpha_j)\cdot\Gamma_\phi\cdot D_\phi$ можно представить как $B(\alpha_j)\Gamma_\phi\cdot D_\phi = h(1,x,x^2,\ldots,x^{d-2})^T$, и, следовательно, матрицу $B\cdot\Gamma_\phi\cdot D_\phi$ — в виде $B\cdot\Gamma_\phi\cdot D_\phi = h\cdot B$, где строки невырожденной матрицы $h = \{h_{i,j}\}$ определяются равенством $(ax+b)^{d-2-i}(cx+e)^i = \sum_{i=0}^{d-2} h_{i,j}x^j$. Таким образом, при любом ϕ матрица $\Gamma_\phi\cdot D_\phi$ входит в группу обобщенных автоморфизмов $\Xi_\mathcal{K}$.

Матрицы $\Lambda_\phi = \Gamma_\phi\cdot D_\phi$ образуют группу изоморфную группе Φ_q. Для того, чтобы это проверить, заметим, что $\Gamma_\phi^{-1}\cdot D_{\phi'}\cdot\Gamma_\phi = \mathrm{diag}((c'\phi(\alpha_1)+e')^{d-2}, \ldots, (c'\phi(\alpha_n)+e')^{d-2}) = D_{\phi',\phi}$, если $\phi'(x) = \frac{a'x+b'}{c'x+e'}$. Отсюда $D_{\phi'}\cdot\Gamma_\phi = \Gamma_\phi\cdot D_{\phi',\phi}$. Следовательно, $\Gamma_{\phi'}\cdot D_{\phi'}\cdot\Gamma_\phi\cdot D_\phi = \Gamma_{\phi'\otimes\phi}\cdot D_{\phi',\phi}\cdot D_\phi$. Прямая выкладка показывает, что $D_{\phi',\phi}\cdot D_\phi = D_{\phi'\otimes\phi}$, т.е. группа, образованная матрицами $\Gamma_\phi\cdot D_\phi$, изоморфна дробно-линейной группе Φ_q. Теорема доказана.

Этот результат будет использован при анализе стойкости системы открытого шифрования, построенной с помощью кода Рида-Соломона (см. §4).

Группа $\Xi_\mathcal{K}$ обобщенных автоморфизмов кода Рида-Соломона также является трижды транзитивной в следующем смысле. Для любой пары упорядоченных троек из попарно различных элементов $(\beta_1,\beta_2,\beta_3)$ и $(\gamma_1,\gamma_2,\gamma_3)$, где $\{\beta_1,\beta_2,\beta_3\}$, $\{\gamma_1,\gamma_2,\gamma_3\} \in \mathfrak{A} = \{\alpha_1,\alpha_2,\ldots,\alpha_n\} = \mathbf{F}'_q$ существует такая унипотентная матрица $\Lambda_\phi \in \Xi_\mathcal{K}$, которая переводит координаты $x_{\beta_1}, x_{\beta_2}, x_{\beta_3}$ вектора $\mathbf{x} = (x_{\alpha_1}, x_{\alpha_2}, \ldots, x_{\alpha_n})$ в координаты $x_{\gamma_1}, x_{\gamma_2}, x_{\gamma_3}$ вектора $\mathbf{x}\Lambda_\phi$ с умножением их на соответствующие постоянные, определяемые диагональной матрицей $D_\phi = \mathrm{diag}(d_{\alpha_1}, d_{\alpha_2}, \ldots, d_{\alpha_n})$. Например, с помощью подходящей матрицы Λ_ϕ можно передвинуть на первые три места любые три координаты вектора $\mathbf{x}$. В частности, если $\{\beta_1 = 1, \beta_2 = 0, \beta_3 = \infty\}$ и $\gamma_1 = \alpha_1, \gamma_2 = \alpha_2, \gamma_3 = \alpha_3$, то $\mathbf{x}\Lambda_\phi = (d_{\alpha_1}x_1, d_{\alpha_2}x_0, d_{\alpha_3}x_\infty, d_{\alpha_4}x_{\phi(\alpha_4)}, \ldots, d_{\alpha_n}x_{\phi(\alpha_n)})$ для некоторой подходящей функции $\phi(x)$.

2. Декодирование

Мы приведем без доказательства ряд утверждений о декодировании кодов, которые будут играть центральную роль при обосновании стойкости рассматриваемых систем открытого шифрования.

Неформально говоря, под термином "декодирование" понимается алгоритм, который позволяет по искаженному ошибками кодовому вектору $\mathbf{a}'$ восстановить исходный кодовый вектор $\mathbf{a}$. Таким образом, декодирование сводится к решению уравнения

$$\mathbf{a}' = \mathbf{a} + \mathbf{e},\ \mathbf{a} \in \mathcal{K},\ \ wt(\mathbf{e}) \leq t, \tag{12}$$

где неизвестными являются кодовый вектор $\mathbf{a}$ и вектор ошибки $\mathbf{e}$.

Имеется несколько различных типов декодирования.

i. *Корреляционное декодирование кода $\mathcal{K}$.* Это алгоритм, который по предъявленному вектору $\mathbf{x} \in \mathbf{F}_q^n$ находит один или несколько кодовых векторов $\mathbf{a} \in \mathcal{K}$, ближайших (в метрике Хемминга) к $\mathbf{x}$.

ii. *Декодирование кода $\mathcal{K}$ в пределах его кодового расстояния.* Это алгоритм, который по вектору $\mathbf{x}$, который отстоит от одного из кодовых векторов $\mathcal{K}$ на расстояние $\leq \frac{d(\mathcal{K})-1}{2}$, вычисляет этот ближайший кодовый вектор. Этот вектор обязательно является единственным. Векторы $\mathbf{x}$, которые отстоят от всех кодовых точек на расстояние большее, чем половина кодового расстояния, могут быть декодированы как угодно, в частности, алгоритм может вообще отказаться от их декодирования.

iii. *Декодирование кода $\mathcal{K}$ за пределами его кодового расстояния.* (Алгоритм промежуточного положения между i. и ii.) Это алгоритм, который по вектору $\mathbf{x}$, находящемуся не очень далеко ($d(\mathbf{x}, \mathbf{a}) \leq t'$) от некоторого кодового вектора $\mathbf{a}$ кода $\mathcal{K}$, вычисляет один или несколько кодовых векторов $\mathbf{a}'$, находящихся на расстоянии $\leq t'$ от $\mathbf{x}$, где $t' > \frac{d(\mathcal{K})-1}{2}$ — некоторая постоянная (параметр алгоритма).

Наиболее сильным и трудным для реализации является алгоритм i.. В настоящее время не известно ни одного нетривиального класса кодов, которые имеют алгоритм декодирования этого типа с простой реализацией. Другими словами, этот алгоритм может быть реализован только с помощью перебора. А именно, можно сравнивать $\mathbf{x}$ со всеми векторами кода и выделять среди них ближайшие кодовые векторы, или осуществлять просмотр векторов из окрестности $\mathbf{x}$, пытаясь найти в ней кодовый вектор. Какой из этих упомянутых алгоритмов перебора выгодней с вычислительной точки зрения зависит от соотношений между параметрами кода.

Сложность реализации корреляционного декодирования нетривиальных кодов возрастает как экспоненциальная функция от их длины. На практике ни один из таких кодов на современных вычислительных средствах не может быть декодирован, начиная с длины ≈ 100.

Наиболее легким для реализации является алгоритм декодирования типа ii.. Для большинства, так называемых, алгебраических кодов известны алгоритмы декодирования в пределах их кодового расстояния, сложность которых возрастает как полином небольшой степени от длины кода. К таким кодам относятся и, рассмотренные нами, обобщенные коды Рида-Соломона $RS_q(n, d)$. Их декодирование в пределах кодового расстояния может быть осуществлено не более, чем за $O(n^3)$ операций в поле $\mathbf{F}_q$ [7], [2].

Не надо думать, что для каждого кода существует простой алгоритм декодирования в пределах его кодового расстояния. По современным представлениям такие алгоритмы могут существовать только для кодов, которые снабжены определенной алгебраической или комбинаторной структурой. Вместе с тем у большинства кодов, не очень точно выражаясь, отсутствует в проверочной матрице какая-либо структура, — это коды "общего положения". Примером первого типа кодов является код Рида-Соломона или код Рида-Маллера (совершенно разные коды), а примером второго — код, у которого проверочная матрица выбрана случайно среди всех матриц определенной размерности.

Декодирование в пределах кодового расстояния (типа ii.) некоторых типов кодов общего положения является NP-полной задачей, т.е. предположительно не может быть осуществлено за полиномиальное время от их длины. Более того, общепринято, что

Тезис А. *декодирование последовательности кодов, которые не обладают полезной для декодирования алгебраической или комбинаторной структурой, не может быть осуществлено за полиномиальное время от их длины.*

Это достаточно расплывчатое, но очень правдоподобное утверждение строго не доказано и в настоящее время возможность его доказательства весьма проблематична. Вместе с тем на этом утверждении "держится" обоснование стойкости открытого шифрования на базе кодов, корректирующих ошибки. Мы далее, специально не указывая на это, будем постоянно его придерживаться.

Обычно при построении кода, корректирующих ошибки, стараются наделять его определенной структурой, которая обеспечивает, с одной стороны, заданное значение его кодового расстояния, и, с другой позволяет, осуществлять его декодирование с малой вычислительной сложностью.

Приведем одно почти очевидное утверждение о сложности декодирования любого кода с помощью алгоритма типа ii..

Утверждение 2. *Любой линейный код $\mathcal{K}$ с параметрами $[n,k,d]_r$, $d \le n/2$, имеет алгоритм декодирования в пределах его кодового расстояния, сложность которого не выше* $O(\min(nr^k, n\sum_{j=0}^{t}\binom{n}{j}))$, *где* $t = [\frac{d-1}{2}]$.

Отметим, что r^k — число элементов в коде $\mathcal{K}$ и $O(nr^k)$ — число операций требуемых для перебора всех элементов кода и сравнения каждого из них с искаженным кодовым вектором $\mathbf{a}'$. Далее, $\sum_{j=0}^{t}\binom{n}{j}(r-1)^j$ — число элементов в шаре радиуса t с центром в точке $\mathbf{x}$ и $O(n\sum_{j=0}^{t}\binom{n}{j})$ — число операций, требуемых для перебора всех элементов шара с целью нахождения среди них кодового вектора.

3. Система открытого шифрования на основе кода, корректирующего ошибки

3.1. Система открытого шифрования Маклиса. Идею построения системы открытого шифрования проще всего пояснить на примере кода Боуза-Чоудхури-Хоквингема $BCH_r(n,d)$ размерности k.

Пусть A — фиксированная порождающая матрица обобщенного кода $BCH_r(n,d)$ над $\mathbf{F}_r$, т.е. матрица ранга k и размера $k \times n$, для которой $A \cdot C^T = 0$, где C — матрица, определенная соотношением (8). Между прочим, в качестве A можно взять матрицу, которая имеет тот же вид, что и C. Этот факт мы использовать не будем.

Ансамбль $\mathcal{A}_r(n,d)$ порождающих матриц обобщенного кода $BCH_r(n,d)$ определим как множество всех матриц вида $h \cdot A \cdot \Gamma \cdot D$, где h пробегает множество всех невырожденных $k \times k$-матриц над $\mathbf{F}_r$, D — множество всех диагональных матриц с ненулевыми на диагоналями элементами, а Γ — множество всех перестановочных матриц размера $n \times n$. Соответственно, ансамбль кодов $\mathcal{K}_r(n,d)$ определяется как множество всех кодов с порождающими матрицами из ансамбля $\mathcal{A}_r(n,d)$. Матрицы h, Γ, D "маскируют" матрицу A.

Передача секретного сообщения абонента $\mathcal{Y}$, предназначенного абоненту $\mathcal{X}$, предваряется следующими действиями. Абонент $\mathcal{X}$ случайно, равновероятно в соответствующем множестве и независимо от других абонентов выбирает матрицы $h = h_{\mathcal{X}}$, $D = D_{\mathcal{X}}$, $\Gamma = \Gamma_{\mathcal{X}}$ и вычисляет матрицу $A' = A'_{\mathcal{X}} = h_{\mathcal{X}} \cdot A \cdot \Gamma_{\mathcal{X}} \cdot D_{\mathcal{X}}$ из ансамбля $\mathcal{A}_r(n,d)$. Матрица $A'_{\mathcal{X}}$ является открытым (общедоступным для всех абонентов) ключом (public key), а матрицы $h_{\mathcal{X}}, \Gamma_{\mathcal{X}}, D_{\mathcal{X}}$– секретным ключом (private key) абонента $\mathcal{X}$.

Шифрованная информация $\mathbf{b}$ (криптограмма), которую абонент $\mathcal{Y}$ передает по общедоступному каналу абоненту $\mathcal{X}$, в системе Маклиса [1] представляет собой вектор длины n и вида $\mathbf{b} = \vec{a}A'_{\mathcal{X}} + \mathbf{e}$, где $\vec{a}$ — $r-$значный вектор длины k, несущий конфиденциальную информацию абонента $\mathcal{Y}$, а $\mathbf{e}$ — секретный вектор ошибок веса, не превосходящего t, и длины n, который случайно и равновероятно выбирается абонентом $\mathcal{Y}$ среди всех векторов веса не выше t.

Таким образом, для того чтобы расколоть открытую информацию необходимо представить вектор $\mathbf{b}$ в виде

$$\mathbf{b} = \mathbf{a} + \mathbf{e}, \tag{13}$$

где вектор $\mathbf{a} = \vec{a}A'_{\mathcal{X}}$ принадлежит коду $K = K_{\mathcal{X}}$ с порождающей матрицей $A'_{\mathcal{X}}$, а вектор $\mathbf{e}$ имеет вес $\le t$.

Другими словами, злоумышленнику необходимо декодировать код K с известной порождающей матрицей $A'_{\mathcal{X}}$. Матрица $A'_{\mathcal{X}}$ замаскирована матрицами h, D и Γ и поэтому она, вообще говоря, представляется нападающей стороне как матрица общего положения. По тезису А в этом случае сложность декодирования не является полиномиальной от длины n кода K. Следовательно, при достаточно больших n процедура декодирования недоступна для злоумышленника из-за ее большой вычислительной сложности. Вместе с тем декодирование кода K той же длины n для легитимного абонента $\mathcal{X}$, знающего секретный ключ, является вычислительно достижимым.

Действительно, абонент $\mathcal{X}$, получив вектор $\mathbf{b}$, восстанавливает кодовый вектор $\vec{a}A'_{\mathcal{X}}$ следующим образом. Сначала он строит вектор $\mathbf{b}' = \mathbf{b}D^{-1} \cdot \Gamma^{-1}$, который , очевидно, является вектором кода

$BCH_r(n,d)$ с порождающей матрицей A, искаженный не более, чем в t разрядах. Как раз здесь используется тот факт, что унипотентная матрица $D^{-1}\cdot\Gamma^{-1}$ сохраняет вес вектора $\mathbf{e}$ (см. раздел 1.9). Затем с помощью какого–либо общеизвестного полиномиального алгоритма декодирования кода $BCH_r(n,d)$ находится вектор $\vec{a}'$, который удовлетворяет условию $\mathbf{b}'=\vec{a}'A+\mathbf{e}'$, где $w(\mathbf{e}')\le t$. Затем вычисляется вектор $\vec{a}$ в виде $\vec{a}=\vec{a}'h^{-1}$.

Мы будем предполагать, что $t\le(d-1)/2$. Вместе с тем можно полагать, что $t>d-1)/2$, но t меньше некоторой границы. При этом надо использовать алгоритм декодирования работы [5] или работы [], которые работают при определенном ограничении на величину t "почти всегда" правильно. Как будет видно ниже, чем больше алгоритм декодирования исправляет ошибок, тем выше будет стойкость системы шифрования. Вместе с тем при возрастании числа исправляемых ошибок, как правило, возрастает и сложность его реализации. В идеале, лучше всего использовать корреляционный алгоритм, но его сложность является слишком высокой и он не доступен для реализации. Обычно в системе Маклиса используют алгоритмы типа ii. или iii..

3.2. Система открытого шифрования Нидеррайтера. В системе Нидеррайтера [4] рассматривается ансамбль $\mathcal{B}_r(n,d)$ проверочных матриц кода $BCH_r(n,d)$, который определяется как множество всех матриц вида $B'=h\cdot C\cdot D\cdot\Gamma$, где C — фиксированная проверочная матрица вида (8), h пробегает множество всех невырожденных $n-k\times n-k$-матриц над $\mathbf{F}_r$, D — множество всех диагональных матриц с ненулевыми на диагонали элементами, а Γ — множество всех перестановочных матриц размера $n\times n$.

Подобно системе Маклиса открытым ключом абонента $\mathcal{X}$ в системе Нидеррайтера является матрица B', а секретным — матрицы h, D, Γ.

Шифрованная информация $\mathbf{c}$ абонента $\mathcal{Y}$ и предназначенная абоненту $\mathcal{X}$ в системе Нидеррайтера представляет собой r-значный длины $n-k$ и вида

$$\mathbf{c}=\mathbf{e}{B'}^T, \tag{14}$$

где $B'=B'_{\mathcal{X}}$ проверочная матрица, которая случайно выбрана абонентом $\mathcal{X}$ из ансамбля $\mathcal{B}_r(n,d)$ и k — размерность кода с этой проверочной матрицей. Вектор $\mathbf{e}$ является вектором длины n и веса, не превосходящего t, который несет конфиденциальную информацию абонента $\mathcal{Y}$.

Заметим, что конфиденциальная информация является одним из решений уравнения

$$\mathbf{c}=\mathbf{x}{B'}^T. \tag{15}$$

Найти какое-либо решение этого уравнения простая задача — это линейное уравнение с $n-k$ уравнениями и n неизвестными. Найти среди всех решений (их число 2^k) решение с минимальным весом это уже сложная задача, которая эквивалентна задаче декодирования кода с проверочной матрицей B'. Доказательство последнего утверждения просто. Если мы умеем находить решение $\mathbf{e}$ уравнения (15) минимального веса, то решение уравнения (12) производится следующим образом. Сначала вычислим вектор $\mathbf{a}'{B'}^T=\mathbf{e}{B'}^T$ (синдром $\mathbf{a}'$), найдем вектор ошибок $\mathbf{e}$, а затем и кодовый вектор $\mathbf{a}=\mathbf{a}'-\mathbf{e}$.

Также как в системе Маклиса в системе Нидеррайтера матрица B' представляется нападающей стороне матрицей общего положения.

В теории кодирования вектор $\mathbf{c}$ из (14) называют синдромом вектора $\mathbf{e}$. Отметим, что матрицы B' и A' связаны соотношением $B'\cdot{A'}^T=0$, где A' — одна из матриц ансамбля $\mathcal{A}_r(n,d)$. Строки матрицы B' являются базисом подпространства размерности $N-k$ ортогонального к пространству строк матрицы A'.

Абонент $\mathcal{X}$, получив сообщение $\mathbf{c}$, находит какой–либо вектор $\mathbf{b}$, который является решением уравнения $\mathbf{x}{B'}^T=\mathbf{c}$. Очевидно, вектор $\mathbf{b}$ является вектором вида $\mathbf{b}=\vec{a}A'+\mathbf{e}$ при некотором неизвестном $\vec{a}\in\mathbf{F}_r^k$. Затем абонент $\mathcal{X}$ также, как в системе Маклиса, декодирует вектор $\mathbf{b}\Gamma^{-1}\cdot D^{-1}=\mathbf{b}'=\vec{a}'A+\mathbf{e}'$, но вместо кодового вектора $\vec{a}'A$ находит вектор $\mathbf{e}'=\mathbf{b}'-\vec{a}'A$, а затем и вектор $\mathbf{e}=\mathbf{e}'\Gamma\cdot D$. Отметим, что в отличие от системы Маклиса, в системе при расшифровании (восстановлении вектора $\mathbf{e}$) никак не участвует матрица h. Она нужна только для маскировки матрицы B'.

Как и выше, предполагаем, что используемый алгоритм декодирования кода $BCH_r(n,d)$ всегда правильно восстанавливает вектор ошибок $\mathbf{e}$.

3.3. Сравнение систем открытого шифрования Маклиса и Нидеррайтера. Системы Маклиса и Нидеррайтера обладают одинаковой стойкостью к нападению, ибо криптографическая атака на одну из систем может быть легко трансформирована в атаку на другую. Поясним это подробно.

Мы полагаем, что обе взаимно ортогональные матрицы A' (открытый ключ системы Маклиса) и B' (открытый ключ системы Нидеррайтера) известны нападающей стороне, так как одна из другой может быть получена как решение линейной системы уравнений $A' \cdot B'^T = 0$, т.е. с помощью не более, чем $O(n^3)$ операций.

При известном синдроме $\mathbf{c} = \mathbf{e}B'^T$ нетрудно вычислить вектор $\mathbf{b} = \vec{a}A' + \mathbf{e}$ с некоторым вектором $\vec{a} \in \mathbf{F}_r^k$ такой, что $\mathbf{c} = \mathbf{b}B'^T$. Для этого надо найти какое-либо решение $\mathbf{b}$ уравнения (15). Вектор $\mathbf{b}$ мы будем рассматривать как криптограмму в системе Маклиса. Если для системы Маклиса найдена криптографическая атака со сложностью Q, т.е. известен алгоритм вычисления вектора $\vec{a}$ (конфиденциальная информация в системе Маклиса), то вектор $\mathbf{e}$ (конфиденциальная информация в системе Нидеррайтера), очевидно, представляется в виде $\mathbf{e} = \mathbf{b} - \vec{a}A'$, т.е. сложность определения $\mathbf{e}$, по существу, совпадает со сложностью определения $\vec{a}$.

Наоборот, если для системы Нидеррайтера известна криптографическая атака со сложностью Q, то используя в качестве криптограммы этой системы вектор $\mathbf{c} = \mathbf{b}B'^T = (\vec{a}A' + \mathbf{e})B'^T = \mathbf{e}B'^T$, где $\mathbf{b}$ — криптограмма системы Маклиса, вычислим вектор ошибок $\mathbf{e}$, а затем и вектор $\vec{a}$, который является единственным решением линейного уравнения $\vec{y}A' = \mathbf{b} - \mathbf{e}$.

Соображения, использованные в предыдущих двух абзацах, любезно сообщены автору в устной беседе Г.А. Кабатянским.

3.4. Некоторые свойства систем открытого шифрования Маклиса и Нидеррайтера. Две эти системы различаются скоростью передачи. Если код $\mathcal{K}$ является низкоскоростным, т.е. k/n — малое число, то скорость передачи у системы Нидеррайтера всегда выше по сравнению с системой Маклиса. Поэтому далее будем рассматривать только ее. Вместе с тем будем предполагать, не оговаривая этого особо, что криптограммой системы Нидеррайтера является n-мерный вектор $\mathbf{b} = \vec{a}A' + \mathbf{e}$, который является каким–либо решением системы (15), где $\mathbf{c} = \mathbf{b}B'^T = \mathbf{e}B'^T$ и $\mathbf{e}$ — вектор веса не выше t (информационный вектор абонента $\mathcal{Y}$). Это связано с тем, что алгоритм декодирования кода $RS_q(n,d)$, рассмотренный в [5], и некоторые известные криптографические атаки оперируют с искаженным кодовым вектором $\mathbf{b}$, а не с его синдромом $\mathbf{c}$.

Шифрование сообщения $\mathbf{e}$ состоит в вычислению его синдрома и поэтому его сложность шифрования равна $O((N-k)N)$ операций. Сложность расшифрования (сложность восстановления вектора $\mathbf{e}$) определяется, в основном, трудоемкостью алгоритма декодирования кода $RS_q(n,d)$ и при использовании алгоритма декодирования работы [5] не превосходит $O(n^3)$ операций. Для декодирования в пределах кодового расстояния известны и более быстрые алгоритмы (см. [],[]).

Как известно [8], кодовые системы открытого шифрования имеют большую скорость шифрования по сравнению с другими подобными системами, например, с системой RSA. Вместе с тем они обладают, по меньшей мере, двумя недостатками.

Во–первых, скорость передачи у кодовой системы всегда меньше 1 (обычно меньше 1/2), в то время как в системе RSA (см. [9] и многие другие работы) она равна 1.

Во–вторых, открытый ключ (в рассматриваемой кодовой системе — матрица B') имеет объем примерно в $n-k$ раз больший, чем у упомянутой системы RSA. Если k относительно маленькое число то выгодней в качестве открытого ключа системы рассматривать матрицу A', которая связана с B' соотношением $B' \cdot A' = 0$.

Кроме того работ по оценке стойкости кодовых систем известно значительно меньше, чем для системы RSA.

В системе открытого шифрования Нидеррайтера в качестве открытой информации выступают векторы $\mathbf{e}$ веса t и менее. Для ее реализации необходимо иметь алгоритм, который отображает множество всех r-значных векторов длины s в множество W_t векторов длины n и веса не выше t, где $s \le \tau(t,N) = [\lg_r \sum_{i=0}^{t} \binom{N}{i}(r-1)^i]$ (логарифм числа возможных сообщений в системе Нидеррайтера). Этого относительно простого вопроса мы касаться не будем.

Система Нидеррайтера полностью определяется как проверочной матрицей B', так и ортогональной к ней порождающей матрицей A', и наоборот. Поэтому открытым ключом этой системы естественно считать матрицу, которая содержит меньшее число строк, хотя криптограмма $\mathbf{c} = \mathbf{e}B'$ всегда реально строится с помощью матрицы B'.

Переход от системы Маклиса к системе Нидеррайтера полезен не только с точки зрения повышения скорости передачи, но и, что, возможно, более важно, позволяет с помощью несложной модернизации существенно усилить ее стойкость к криптографическим атакам. По поводу этого вопроса см. работу [3].

4. Как раскалывается система открытого шифрования Нидеррайтера, построенная с помощью обобщенного кода Рида-Соломона ? Общие подходы.

В этом разделе мы рассматриваем систему Нидеррайтера, построенную с помощью q-значного кода из ансамбля $\mathcal{B}_q(n,d)$ (см. начало раздела 3.2). Как было установлено в разделе 3.3, соответствующая система Маклиса (система, в которой порождающие матрицы выбираются из ансамбля $\mathcal{A}_q(n,n-d+1)$ имеет примерно ту же стойкость к нападению, что и рассматриваемая система открытого шифрования.

Имеется два вида атак на систему открытого шифрования.

i. "Чтение" открытого сообщения абонента $\mathcal{Y}$ без использования секретного ключа абонента $\mathcal{X}$ (бесключевое чтение). В данном случае секретным ключом являются матрицы h, Γ, D.

ii. Вычисление секретного ключа абонента $\mathcal{X}$ с последующим вычислением открытых сообщений абонента $\mathcal{Y}$, направляемых им абоненту $\mathcal{X}$.

Рассмотрим сначала атаку i.. Для ее реализации необходимо решить уравнение (15). С точки зрения нападающей стороны матрица B' является матрицей общего положения. Поэтому для нахождения решения $\mathbf{e}$ уравнения (15) веса $wt(\mathbf{e}) \le t$ в соответствие с тезисом А необходимо проделать экспоненциальное от его длины n число операций. Можно полагать, что при большем $n \approx 100$ это не возможно на современном уровне развития вычислительной техники.

Другой подход, реализующий атаку i., состоит в следующем. Можно "угадать" обобщенный код Рида-Соломона, определяемый проверочной матрицей B', и произвести декодирование (решить уравнение (15)) в этом коде. По следствию 1 число таких кодов $A_q(n,d)$ не меньше $\frac{n!(q-1)^n}{(q^{d-1}-1)(q^{d-1}-q)\cdots(q^{d-1}-q^{d-2})}$. Это число при $n \approx 100$, $d \le n/2$ и $q \ge 2$ больше, чем 10^{77}. Поэтому это событие очень маловероятно и его можно не рассматривать.

Таким образом, по современным представлением с учетом тезиса А бесключевое чтение (атака i.) в рассматриваемой системе невозможно при достаточно большом n.

Рассмотрим теперь атаку ii.. Задачей в этом случае является определение матрицы h, Γ, D, исходя из известной матрице B'. Как будет показано ниже и это основной результат работы эта задача может быть решена за $O(s^4 + sn)$ операций в поле $\mathbf{F}_q$.

5. Алгоритм определения секретного ключа системы открытого шифрования, использующего обобщенный код Рида-Соломона

Любая матрица ансамбля $\mathcal{B}_q(n,d)$ имеет вид

$$B' = \begin{pmatrix} z_1 f_0(\omega_1) & z_2 f_0(\omega_2) & \cdots & z_n f_0(\omega_n) \\ z_1 f_1(\omega_1) & z_2 f_1(\omega_2) & \cdots & z_n f_1(\omega_n) \\ z_1 f_2(\omega_1) & z_2 f_2(\omega_2) & \cdots & z_n f_2(\omega_n) \\ \vdots & \vdots & \cdots & \vdots \\ z_1 f_{d-2}(\omega_1) & z_2 f_{d-2}(\omega_2) & \cdots & z_n f_{d-2}(\omega_n) \end{pmatrix}, \tag{16}$$

где $f_i(x)$ многочлен степени не выше $d-2$, который определяются матрицей $h = \{h_{i,j}\}$ следующим образом $f_i(x) = \sum_{j=0}^{d-2} h_{i,j}$. Многочлены $f_i(x)$ являются линейно-независимыми.

Итак, перед нами стоит задача: по заданной матрице B' найти невырожденную матрицу h, элементы $\omega_1, \omega_2, \dots, \omega_n \in \mathbf{F}'_q = \mathbf{F}_q \cup \{\infty\}$ и элементы $z_1, z_2, \dots, z_n \in \mathbf{F}_q \setminus \{0\}$ такие, что $B' = h \cdot B \cdot \Gamma \cdot D$, $D = \mathrm{diag}(z_1, z_2, \dots, z_n)$.

Задачу будем решать в два этапа: сначала найдем элементы $\omega_1, \omega_2, \dots, \omega_n$, а затем элементы $z_1, z_2, \dots, z_n$ и матрицу h.

5.1. Как определить первые три элемента ω_j? Перед тем как искать элементы $\omega_1, \omega_2, \dots, \omega_n$ сделаем несколько замечаний.

Пусть h, Λ — некоторое решение уравнения (16), т.е. $B' = h \cdot B \cdot \Lambda$, $\Lambda = \Gamma \cdot D$, и $\Lambda_\phi = \Gamma_\phi \cdot D_\phi$, $D_\phi = \mathrm{diag}(z'_1, z'_2, \dots, z'_n)$, — некоторый обобщенный автоморфизм кода $\mathcal{K}$ с порождающей матрицей B (см. 8), соответствующий дробно-линейной функции $\phi(x)$ (см. раздел 1.10). Тогда решением уравнения (16) является также пара h', Λ', где $h' = h \cdot {h''}^{-1}$, $\Lambda' = \Lambda_\phi \cdot \Lambda$, где матрица h'' определяется соотношением $h'' \cdot B = B \cdot \Lambda_\phi$.

Группа обобщенных автоморфизмов $\Xi_{\mathcal{K}}$ кода $\mathcal{K} = RS_q(n,d)$ Рида-Соломона типа 3 (см. раздел 1.4) действует на координатах векторов $\mathbf{x} = (x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n})$. Она образована всеми унипотентными матрицами Λ_ϕ (теорема 2) и является трижды транзитивной. Смысл этого понятия объяснен в разделе 1.10. Поэтому найдется дробно-линейная функция $\phi(x)$ такая, что

$$h' \cdot B \cdot \Lambda_\phi \cdot \Lambda = \begin{pmatrix} z_1'' f_0'(1) & z_2'' f_0'(0) & z_3'' f_0'(\infty) & \cdots & z_n'' f_0'(\beta_n) \\ z_1'' f_1'(1) & z_2'' f_1'(0) & z_3'' f_1'(\infty) & \cdots & z_n'' f_1'(\beta_n) \\ z_1'' f_2'(1) & z_2'' f_2'(0) & z_3'' f_2'(\infty) & \cdots & z_n'' f_2'(\beta_n) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ z_1'' f_{d-2}'(1) & z_2'' f_{d-2}'(0) & z_3'' f_{d-2}'(\infty) & \cdots & z_n'' f_{d-2}'(\beta_n) \end{pmatrix}, \tag{17}$$

Т.е. найдется такая матрица $\Lambda_\phi \cdot \Lambda$, что $(x_{\omega_1}, x_{\omega_2}, \dots, x_{\omega_n})\Lambda_\phi \cdot \Lambda = (d_1 x_1, d_2 x_0, d_3 x_\infty, \beta_4, \dots, \beta_n)$, где d_ω — элементы диагональной матрицы D', определяемой соотношением $\Lambda_\phi \cdot \Lambda = \Lambda' = \Gamma' \cdot D'$ (см. раздел 1.10).

Для этого, как нетрудно видеть, нужно подобрать такую функцию $\phi(x)$, что $\phi(\omega_1) = \beta_1,\ \phi(\omega_2) = \beta_2,\ \phi(\omega_3) = \beta_3$, где элементы β_i определяются тем условием, что матрица Λ переводит координату x_{β_1} в координату x_1, координату x_{β_2} в x_0 и координату x_{β_3} в x_∞.

Таким образом, всегда можно полагать, что в (16) $\omega_1 = 1,\ \omega_2 = 0,\ \omega_3 = \infty$.

5.2. Определение элементов $\omega_j,\ j > 3$. Найдем такие постоянные $c_s^{(1)},\ s = 0, \dots, d-2$, не все равные нулю, для которых выполнено

$$\sum_{s=0}^{d-2} c_s^{(1)} z_j f_s(\omega_j) = 0,\ j = 1, d, d+1, \dots, 2d-4. \tag{18}$$

Для этого необходимо решить однородную систему линейных уравнений от $d-1$ неизвестных с известной матрицей коэффициентов $(z_j f_s(\omega_j))$ — части матрицы B'. Эта система всегда имеет решение, так как уравнений меньше, чем число неизвестных.

Следует отметить, что все элементы $c_s^{(1)}$ отличны от нуля, так как в противном случае в матрице B' нашлись бы $d-1$ линейно-зависимых столбцов, что по ее построению не может иметь место.

Положим

$$F^{(1)}(x) = \sum_{s=0}^{d-2} c_s^{(1)} f_s(x),\ \ \gamma_i^{(1)} = \sum_{s=0}^{d-2} c_s^{(1)} z_i f_s(\omega_i) = z_i F^{(1)}(\omega_i). \tag{19}$$

Очень существенно то, что элементы $\gamma_i^{(1)}$ могут быть вычислены, исходя только из известных элементов $z_i f_s(\omega_i)$ матрицы B'.

Поскольку элементы z_i отличны от нуля, то из (19) следует, что элементы $\omega_j,\ j = 1, d, d+1, \dots, 2d-4$ являются корнями многочлена $F^{(1)}(x)$. Заметим, что ни один из элементов $\omega_1, \omega_d, \omega_{d+1}, \dots, \omega_{2d-4}$ не равен ∞, так как $\omega_3 = \infty$.

Степень многочлена $F^{(1)}(x)$ не превосходит $d-2$, так как степени $f_j(x)$, из которых он составлен, также не превосходят $d-2$. Кроме того, многочлен $F^{(1)}(x)$ не равен тождественно 0, ибо многочлены $f_s(x)$ линейно-независимы, а коэффициенты $c_s^{(1)}$ все отличны от нуля. Отсюда вытекает, что $F^{(1)}(x) = a^{(1)}(x-1)(x-\omega_d)\cdots(x-\omega_{2d-4}),\ a^{(1)} \neq 0$.

Отметим, что $F^{(1)}(\omega) \neq 0$, если $\omega \neq \omega_j,\ j = 1, d, d+1, \dots, 2d-4,\ \omega \neq \infty$ и $F^{(1)}(\infty) = a^{(1)}$.

Теперь проделаем ту же процедуру для элементов $\omega_j,\ j = 2, d, d+1, \dots, 2d-4$.. А именно, найдем такие постоянные $c_s^{(2)},\ s = 0, \dots, d-2$, не все равные нулю, для которых выполнено

$$\sum_{s=0}^{d-2} c_s^{(2)} f_s(\omega_j) = 0,\ j = 2, d, d+1, \dots, 2d-4. \tag{20}$$

Положим

$$F^{(2)}(x) = \sum_{s=0}^{d-2} c_s^{(2)} f_s(x),\ \gamma_i^{(2)} = \sum_{s=0}^{d-2} c_s^{(2)} z_i f_s(\omega_i) = z_i F^{(2)}(\omega_i). \tag{21}$$

По тем же соображениям, что и выше, имеем $F^{(2)}(x) = a^{(2)} x(x-\omega_d)\cdots(x-\omega_{2d-4}),\ a^{(1)} \neq 0$.

Рассмотрим отношение $\theta(x) = \frac{F^{(1)}(x)}{F^{(2)}(x)} = \frac{a^{(1)}(x-1)}{a^{(2)}x}$ многочленов $F^{(1)}(x)$ и $F^{(2)}(x)$. Как уже было замечено, $F^{(i)}(\omega) \neq 0$, $i = 1, 2$, если $\omega \neq \omega_j$, $j = 1, 2, d, d+1, \ldots, 2d-4$, $\omega \neq \infty$. Таким образом, мы можем вычислить значение функции $\theta(x)$ во всех точках ω_j за исключением $j = d, d+1, \ldots, 2d-4$ с точностью до постоянного множителя $\frac{a^{(1)}}{a^{(2)}}$.

Множитель $\frac{a^{(1)}}{a^{(2)}}$ можно вычислить, если положить $x = \infty$ (значению ω_3) в $\theta(x)$. В этом случае $z_3 F^{(i)}(\infty) = \sum_{s=0}^{d-2} c_s^{(i)} z_3 f_s(\infty)$, $i = 1, 2$. Таким образом, значение $\theta(\infty)$ может быть вычислено непосредственно, исходя из матрицы B', ибо $z_3 f_s(\infty)$ — элементы третьего столбца B'. Для полноты изложения заметим, что $F^{(i)}(\infty) \neq 0$, ибо по построению среди всех $d-2$ корней многочлена $F^{(i)}(x)$, степени не выше $d-2$, нет корня ∞. Отсюда вытекает, что

$$\theta(x) = \frac{F^{(1)}(\infty)}{F^{(2)}(\infty)} \left(\frac{x-1}{x} \right) \tag{22}$$

Как уже отмечалось, значения многочленов $F^{(i)}(x)$ и, следовательно, значение $e_\omega = \theta(\omega)$ дробно-линейной функции $\theta(x)$ можно вычислить в любой точке $\omega \in \mathbf{F}'_q$ за исключением $\omega \neq \omega_j$, $j = 1, 2, d, d+1, \ldots, 2d-4$, $\omega \neq \infty$. Отсюда вытекает, что

$$\omega_j = \theta^{-1}(e_{\omega_j}), \quad j \neq 1, 2, 3, d, d+1, \ldots, 2d-4 \tag{23}$$

Заметим, впрочем, что элементы ω_i, $i = 1, 2, 3$, уже известны.

Функция $\theta^{-1}(x)$, как нетрудно вычислить, равна $\theta^{-1}(x) = \frac{F^{(1)}(\infty)}{F^{(1)}(\infty) - xF^{(2)}(\infty)}$. Таким образом, мы можем определить значения ω_j для всех j, исключая $j = d, d+1, \ldots, 2d-4$.

Недостающие ω_j можно определить, если выбрать другие элементы, определяющие многочлены $F^{(i)}(x)$. Скажем, в качестве такого набора для определения $F^{(1)}(x)$ можно взять элементы $1, \omega_{2d-3}, \omega_{2d-2}, \ldots, \omega_{3d-6}$ и с их помощью вычислить недостающие ω_j, $j = d, d+1, \ldots, 2d-4$.

В этой секции с помощью многочленов $F^{(i)}(x)$ произведена самая основная и трудная работа: найдена первая часть ключа — элементы ω_j для всех j. Вся остальная работа по определению оставшейся части ключа, как это и обычно бывает, является более легкой и может быть произведена различными способами, один из которых излагается ниже. Кроме того заметим, что мы использовали нетривиальные свойства подгруппы группы автоморфизмов кода Рида-Соломона, а именно ее трижды транзитивность. Если бы подгруппа была только дважды транзитивной, то мы, например не смогли бы вычислить множитель $\frac{a^{(1)}}{a^{(2)}}$ и, следовательно, вычислить все ω_j.

Трудозатраты этой части алгоритма, как нетрудно подсчитать, не больше $O(d^3 + dn)$. Детального обоснования этой оценки производить не будем.

5.3. Определение элементов z_j и матрицы h. Заметим, что если каждый элемент матрицы Λ умножить на $a \in \mathbf{F}_q \setminus \{0\}$, а каждый элемент h на a^{-1}, то произведение $B' = h \cdot B \cdot \Lambda$ останется неизменным. Поэтому можно считать, что $z_1 = 1$.

Найдем такие элементы $c_1, c_2, \ldots, c_d$, что

$$\sum_{s=1}^{d} c_s z_s f_j(\omega_s) = 0, \quad j = 0, \ldots, d-2. \tag{24}$$

Отметим, что все элементы $c_1, c_2, \ldots, c_d$ отличны от нуля, поскольку в противном случае код с проверочной матрицей B' имел бы кодовое расстояние меньшее d (см. раздел 1.3, утверждение 1).

Соотношение (24) в матричной форме имеет вид

$$B''_d \cdot \mathrm{diag}(z_1, z_2, \ldots, z_d)(c_1, c_2, \ldots, c_d)^T = 0, \tag{25}$$

где $B''_d = (f_i(\omega_j))$, $i = 0, 1, \ldots, d-2$, $j = 1, 2, \ldots, d$ — матрица размера $d-1 \times d$. Заметим, что матрица $B''_d \cdot \mathrm{diag}(z_1, z_2, \ldots, z_d)$ является матрицей, совпадающей с первыми d столбцами матрицы B'.

Как нетрудно видеть $B''_d = h \cdot B_d$, где

$$B_d = \begin{pmatrix} \omega_1^0 & \omega_2^0 & \cdots & \omega_d^0 \\ \omega_1 & \omega_2 & \cdots & \omega_d \\ \omega_1^2 & \omega_2^2 & \cdots & \omega_d^2 \\ \vdots & \vdots & \cdots & \vdots \\ \omega_1^{d-2} & \omega_2^{d-2} & \cdots & \omega_d^{d-2} \end{pmatrix} \tag{26}$$

Откуда и из (25) вытекает, что

$$h \cdot B_d \cdot \cdot \mathrm{diag}(z_1, z_2, \ldots, z_d)(c_1, c_2, \ldots, c_d)^T = 0, \tag{27}$$

или

$$B_d \cdot \mathrm{diag}(c_1, c_2, \ldots, c_d) \cdot (z_1, z_2, \ldots, z_d)^T = 0. \tag{28}$$

Соотношение (28) мы будем рассматривать как линейную систему уравнений относительно неизвестных $z_2, z_3, \ldots, z_d$ с учетом того, что ненулевые элементы $c_1, c_2, \ldots, c_d$ и элементы $\omega_1, \omega_2, \ldots, \omega_d$ уже известны, а $z_1 = 1$. Эта система имеет единственное решение, поскольку ее матрица ее коэффициентов

$$\begin{pmatrix} \omega_2^0 & \omega_3^0 & \cdots & \omega_d^0 \\ \omega_2 & \omega_3 & \cdots & \omega_d \\ \omega_2^2 & \omega_3^2 & \cdots & \omega_d^2 \\ \vdots & \vdots & \cdots & \vdots \\ \omega_2^{d-2} & \omega_3^{d-2} & \cdots & \omega_d^{d-2} \end{pmatrix} \cdot \mathrm{diag}(c_2, c_3, \ldots, c_d) \tag{29}$$

является, очевидно, невырожденной. Решая эту систему, найдем элементы $z_1, z_2, \ldots, z_d$.

Найдем теперь элементы матрицы $h = (h_{i,j})$, $i, j = 0, \ldots, d-2$. Имеем

$$z_j \sum_{s=0}^{d-2} h_{i,s} \omega_j^s = z_j f_i(\omega_j). \tag{30}$$

Зафиксировав какое-либо i, $0 \le i \le d-2$, и изменяя j от 1 до $d-1$, получим систему линейных уравнений с неизвестными $h_{i,0}, h_{i,1}, \ldots, h_{i,d-2}$. Определитель этой системы является определителем Вандермонда, поэтому ее решение $h_{i,0}, h_{i,1}, \ldots, h_{i,d-2}$ находится однозначно. Решив эту систему для каждого i мы найдем матрицу h.

Таким образом, мы сумели определить матрицу h, элементы $\omega_1, \omega_2, \ldots, \omega_d$ и элементы $z_1, z_2, \ldots, z_d$. Для того чтобы определить оставшиеся элементы $z_{d+1}, z_{d+2}, \ldots, z_n$ проще всего поступить следующим образом.

Умножим матрицу B' слева на матрицу h^{-1}. В результате получим матрицу

$$h^{-1} \cdot B' = \begin{pmatrix} z_1\omega_1^0 & z_2\omega_2^0 & \cdots & z_n\omega_n^0 \\ z_1\omega_1 & z_2\omega_2 & \cdots & z_n\omega_n \\ z_1\omega_1^2 & z_2\omega_2^2 & \cdots & z_n\omega_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ z_1\omega_1^{d-2} & z_2\omega_2^{d-2} & \cdots & z_n\omega_n^{d-2} \end{pmatrix}, \tag{31}$$

Вид последней матрицы делает задачу определения элементов $z_{d+1}, z_{d+2}, \ldots, z_n$ тривиальной.

Число операций, требуемых для реализации этой части алгоритма по определению оставшейся части ключа (матрицы h и всех элементов z_j) не выше $O(d^4 + dn)$. Таким образом, общее число операций по реализации всего алгоритма не более, чем $O(d^4 + dn)$. Следовательно, сложность этого алгоритма является полиномиальной от длины n используемого кода. Соответствующая система открытого шифрования как Маклиса так и Нидеррайтера, построенная на коде Рида-Соломона, не является стойкой. Это основной результат работы.

5.4. Заключительные замечания. Естественно встает вопрос о модернизации рассмотренной системы шифрования для того, чтобы увеличить ее стойкости. Наиболее естественный путем является выбор для ее построения другого кода — не Рида-Соломона. Напомним, что для использования в системе шифрования подходит только тот код, который имеет легкое декодирование. Таких кодов известно не очень много.

Возможно, подходящим вариантом может послужить обобщенный код Боуза-Чоудхури-Хоквингема длины $n = q + 1$ (см. конец раздела 1.8) над полем $\mathbf{F}_r$, где число r существенно меньше числа q. Нечетко выражаясь, в этом случае построить многочлены $F^{(i)}(x)$ не удается из-за того, матрица h, определенная над $\mathbf{F}_r$, "размазывает" z_j между различными коэффициентами многочленов $f_j(x)$. Имеются и некоторые другие сложности. Вместе с тем у автора имеются основания того, что системы шифрования, построенная на основе обобщенного кода Боуза-Чоудхури-Хоквингема, может быть расколота за полиномиальное время. Исследование криптографических свойств такой системы является достаточно хорошим направлением для самостоятельной работы.

Другим направлением является использование в системе шифрования двоичных кодов Рида-Маллера. В работе [3] рассмотрена такая система и ее модификации. Проведен подробный анализ ее криптографических свойств. В частности, оценена ее стойкость, которая оказалась высокой.

Третьем направлением являются алгебро-геометрические коды. Эти коды образуют значительно более мощные ансамбли по сравнению с ансамблями, построенными с помощью кода Рида-Соломона. Происходит это из-за того, что мы можем варьировать не только матрицы h и Λ, как в случае использования кода Рида-Соломона, но и вид алгебраической кривой, с помощью которой построен этот код. Это является очень мощным методом маскировки свойств открытого ключа — проверочной матрицы B'.

Несколько неопубликованных работ по этому направлению написаны С. О. Шестаковым.

Четвертым совсем не исследованным направлением является использование каскадных кодов или сверточных кодов. По мнению автора на этом направлении могут быть найдены хорошие системы открытого шифрования. Это направление также является перспективным для самостоятельного исследования.

Литература

[1] R.J. McEliece,"A Public–Key Cryptosystem Based on Algebraic Coding Theory", $pp.114-116$ in DGN Progres Report $42-44$, Jet Propulsi on Lab.,Pasadena, CA, January– February,1978.

[2] Сидельников В.М., О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона, Дискретная математика, т. 4, вып. 3, стр. 57-63, 1992.

[3] Сидельников В.М. Открытое шифрование на основе двоичных кодов Рида-Маллера, Дискретная математика, т.6, вып. 3 ,стр. 3-20 ,1994.

[4] H. Niederreiter. Knapsack–Type Cryptosystems and Algebraic Coding Theory. Probl. Control and Inform. Theory, 1986, V. $15, pp.19-34$.

[5] Сидельников В.М. Декодирование кода Рида-Соломона при числе ошибок, большем $\frac{d-1}{2}$, и нули многочленов нескольких переменных, Пробл. перед. инф. т.30, вып. 3 ,стр. 51-69 ,1994.

[6] Сидельников В.М., Першаков А.С. "Декодирование кодов Рида–Маллера при большом числе ошибок" Пробл. перед. инф. т.28, N3 ,стр. 80-94 ,1992.

[7] Мак–Вильямс Ф.Д., Слоэн Н.Дж. "Теория кодов, исправляющих ошибки". М., Связь, 1979.

[8] Riek J.R. Observations on the Application of Error–Correcting Codes to Pablic Key Encryption. Inter. Carnahan Conf. on Security Technology. $1990, pp.15-18$.

[9] Cryptology and Computational Number Theory. Proc. of Sym. in App. Math. Vol $42, 1989$.

[10] E.R.Berlekamp, R.J. McEliece, H.C.A.van Tilborg,"On the Inherent Intractability of Certain Coding Problem" IEEE Trans. vol.IT$-24, pp384-386, 1978$.

[11] Зайцев Г.В., Зиновьев В.А., Семаков Н.В. Быстрое корреляционное декодирование блочных кодов. Сб. "Кодирование и передача дискретных сообщений в системах связи" М. Наука, 1976, стр.74–85.

[12] Евсеев Г.С. "О сложности декодирования линейных кодов" Пробл. перед. инф. т.19, N 1, 1983.

[13] Крук Е.А. "Границы для сложности декодирования линейных кодов" Пробл. перед. инф. т.25, N 3,стр. $103-107, 1989$.

[14] Бассалыго Л.А.,Зяблов В.В., Пинскер М.С. "Проблемы сложности в теории корректирующих кодов" Пробл. перед. инф. т.13, стр. $5-13, 1977$.

[15] Корякин Ю.Д. Быстрое корреляционное декодирование кодов Рида–Маллера. Пробл. перед. инф. т. 23, вып 2, 1987, стр. 40 – 49.
[16] L.B.Levitin, C.P.Hartman, "A New Approach to the General Minimum Distance Decoding Problem: The zero–neighbors Algorithm" IEEE Trans. vol.IT–31, N3, $pp378 - 384, 1985$.
[17] G.C. Ntafos, G.L. Hakimi, "On The Complexity of Gome Coding Problems" IEEE Trans. vol.IT$-27, pp794 - 796, 1981$.
[18] Coffey J.T.,Goodman R.M. The Complexity of Informatin Get Decoding. IEEE Trans. on Information Theory, vol. IT–36, N5, $pp1031 - 1037, 1990$.
[19] C.M.Adams, H.Meijer, "Security–Related Coments Regarding McEliac's Public–Key Cryptosystem" in Advancts in Cryptology – CRYPTO'87 (Ed. C. Pomerance), pp 224-228, Lecture Notes in Computer Sci.No.293, Heidenberg and New–York: Spinger–Verlag, 1988.
[20] P.J.Lee and E.F.Brickell, "An Observation on the Security of the McEliace Public– Key Cryptosystem" in Advancts in Cryptology – EUROCRYPTO'88 (Ed. C. Gunther), pp 224-228, Lecture Notes in Computer Sci.No.230 ,Heidenberg and New–York: Spinger–Verlag, 1988.
[21] J.G.Leon, "A Probalistic Algorithm for Computing Weights of Large Error–Correcting Codes" IEEE Trans.,vol.IT–34, N 5 , pp.1354-1359, 1988.
[22] Кнут Д. Искусство программирования для ЭВМ. т.3. Сортировка и поиск. М. Мир. 1979.
[23] Ленг С., Алгебра, М. Мир, 1968.
[24] Глухов М.М., Елизаров В.П, Нечаев А.А., Алгебра, часть 2, стр. 344-345, М. 1991.
[25] Петерсон У., Уэлдон Э., Коды, корректирующие ошибки, М. Мир, 1976.