Мкртичян Вячеслав Виталиевич – ФГАНУ НИИ "Спецвузавтоматика"; e-mail: realdeal@bk.ru; 344015, г. Ростов-на-Дону, ул. Малиновского, 72/2, кв. 136; тел.: 88632202486, 89044417791; старший научный сотрудник.

Yevpak Sergey Alexandrovich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: sergej-evpak@yandex.ru; 30/95, Marshal Zhukov avenue, 365 flat, Rostov-on-Don, 344029, Russia; phone: +79094142919; the department of the algebra and discrete mathematics of the faculty of mathematics, mechanics and computer sciences; postgraduate student.

Mkrtichan Vyacheslav Vitalievich – FSSI RI "Spetsvuzavtomatika"; e-mail: realdeal@bk.ru; 72/2, Malinovskogo street, 136 flat, Rostov-on-Don, 344015, Russia; phones: +78632202486, +79044417791; senior researcher.

УДК 517.19

Е.А. Михайлова

СИСТЕМА ЗАЩИТЫ МАК-ЭЛИСА В СЛУЧАЙНЫХ СЕТЯХ НА БАЗЕ СЕТЕВОГО КОДА РИДА-СОЛОМОНА*

Рассматривается задача защищенной от помех и наблюдателя передачи одной и той же информации от одного источника некоторому количеству получателей в сети неизвестной структуры. Задача решается на основе предложенного Кёттером и Кшишангом метода случайного сетевого кодирования. В этом методе сеть представляется графом неизвестной структуры, в узлах которого над пришедшими пакетами совершаются случайные линейные преобразования. В работе построена модель сетевого канала, использующего линейное сетевое кодирование, рассмотрены предложенные Кёттером и Кшишангом подпространственные сетевые коды Рида-Соломона, обеспечивающие эффективную помехоустойчивую передачу данных по такому сетевому каналу. Представлены алгоритмы кодирования и декодирования. Построена новая матричная интерпретация кодирования, приведен соответствующий алгоритм. На базе сетевых кодов Рида-Соломона в их матричной интерпретации построена система защиты с открытым ключом, являющаяся некоторым аналогом известной криптосистемы Мак-Элиса. Целью построенной системы защиты является защищенная передача от одного отправителя, знающего открытый ключ, нескольким получателям, владеющим общим секретным ключом, некоторого одинакового набора данных. Приведены алгоритмы шифрования и расшифрования для построенной системы защиты, доказана теорема о корректности работы алгоритмов. В заключение построена симметричная версия системы защиты, изменены соответствующие алгоритмы, отмечены достоинства и недостатки симметричной версии.

Помехоустойчивое кодирование; сетевые коды Рида-Соломона; случайная линейная сеть; система защиты с открытым ключом; криптосистема Мак-Элиса.

E.A. Mikhailova

MCELICE SECURITY SYSTEM IN RANDOM NETWORK BASED ON REED-SOLOMON NETWORK CODE

The problem of error-correction transmission of the same data from one source to several receivers in wiretapped network of unknown structure is considered. The solution based on random network coding technique provided by Koetter and Kschischang. In this method network represent as an unknown structured graph, where each intermediate node creates a random linear combination of the received data and transmits this random combination. The network channel model, using a linear network coding, is constructed. Network subspace Reed-Solomon codes pro-

* Работа подержана грантом ЮФУ на 2013 год ИТ-213.01-24/2013-147.

vided by Koetter and Kschischang that guaranteed efficient error-correction data transmission are described. Encoding and decoding algorithms are introduced. A new matrix-based interpretation of coding is constructed, appropriate algorithm is given. Public-key security system based on network Reed-Solomon code in matrix version which is an analogue of the well-known McEliece cryptosystem is provided. The purpose of constructed security system is to transmit securely the same data from one source which is know the public key to more receivers which are know the private key. Encoding and decoding algorithms for constructed security system are given, the algorithm-validation theorem is proved. In conclusion the symmetric version of security system is constructed, appropriate algorithms are changed, the advantages and disadvantages of the symmetric version are noted.

Error-correction coding; network Reed-Solomon codes; linear random network; public-key security system; McElise cryptosystem.

1. Введение. Рассматривается проблема защиты информации от помех и наблюдателя. При передаче информации по обычному цифровому каналу применяются методы помехоустойчивого кодирования. Для борьбы с ошибками, возникающими из-за помех, разработано множество кодеков [1]. Помехи могут порождать не только ошибки, но и стирания, для борьбы с которыми применяют специальные методы (см., например, [2, 3]). Для борьбы с несанкционированным доступом используются различные криптографические методы [4], активно разрабатываются кодовые криптосистемы, в частности, аналоги систем защиты Мак-Элиса [5]. Разумеется, эти же методы применимы и для передачи данных по сетям, состоящим из различных каналов связи.

В последние годы интенсивно исследуется проблема распределенной передачи данных по специальным детерминированным и случайным сетям, для решения которой разрабатываются методы сетевого кодирования [6–9]. В этих работах рассматриваются ситуации, когда одного отправителя и нескольких получателей связывает некоторая сеть, которую можно смоделировать графом, в узлах которого над полученными данными производятся линейные комбинации. Для таких сетей решается задача пересылки отправителем одинакового набора информации нескольким получателям. Особый интерес представляют рассмотренные в работах [7, 8] случайные линейной сети, в предположении, что ни отправитель, ни получатели не знают ни структуру сети, ни линейных преобразований в промежуточных узлах.

Теория сетевого кодирования находит широкое практическое применение. В [7] предложено применять детерминированные линейные сети, где известна структура сети и коэффициенты сумм, для передачи данных по компьютерным сетям, в [9] доказано, что данный способ для некоторых графов более быстрый, чем использующийся сейчас, когда промежуточные узлы лишь пересылают принимаемую информацию. Модель случайной линейной сети удобна для передачи данных по линейной сети, когда структура сети неизвестна. В работе [8] отмечено, что ситуация, когда структура сети неизвестна, близка к случаю передачи данных при помощи антенн.

Целью настоящей работы является разработка на базе построенных в [8] сетевых кодов Рида-Соломона матричной интерпретации кодирования и на ее основе кодовой сетевой системы защиты с открытым ключом типа криптосистемы Мак-Элиса.

2. Схема передачи данных по случайной сети. Сетевое кодирование. Для восстановления информации, передаваемой по сети, используется сетевое кодирование. Схема состоит из одного источника, нескольких приемников, которым источник должен передать одинаковую информацию, и некоторого множества промежуточных узлов. Также предполагается, что на выходе источника стоит кодер сети, а на входе приемников – декодеры сети.

Исходная информация представляется в виде информационных векторов длины k над полем Галуа $\mathbb{F}_{q^s}$, где q – степень простого числа. Каждый вектор поступает от источника на вход кодера сетевого канала. Кодер производит преобразования, после которых появляется набор из l векторов длины n, которые одновременно поступают на вход сетевого канала. С векторами, приходящими на некоторый узел, сетевым каналом производятся неизвестные, а потому можно считать, что случайные, линейные комбинации над младшим полем. На выходе сетевого канала у каждого приемника на вход декодера сетевого канала поступает некоторое количество векторов над тем же полем $\mathbb{F}_{q^s}$. Кроме того, предполагается, что на сетевой канал может оказываться влияние в виде шума, порождающее ошибки (введение нового случайного базисного вектора) и стирания (исчезновение некоторого отправленного базисного вектора). Декодер некоторым образом преобразует входящий набор векторов, и выдает один вектор исходной длины k над полем $\mathbb{F}_{q^s}$, который возвращается приемнику. Целью является случай, когда полученные приемниками векторы будут совпадать с отправленным.

Суть метода Кёттера и Кшишанга [8] состоит в том, что если кодер сопоставляет информационному вектору подпространство, и передает по сети его базис, то линейные комбинации в узлах не будут выводить векторы из подпространства. Следует отметить, что из-за случайности линейных комбинаций в узлах может быть получена некоторая порождающая система вложенного в исходное подпространства. Кодек является помехоустойчивым.

Приведем необходимые сведения из [8] о сетевых РС-кодах и выпишем для этих кодов алгоритмы кодирования и декодирования. Рассмотрим конечное поле F_q и его расширение – поле $\mathbb{F}_{q^m}$, которое иногда будет удобно представлять как векторное пространство $\mathbb{F}_q^m$. Это возможно в силу наличия биективного соответствия между ними: $\mathcal{T}: \mathbb{F}_{q^m} \to \mathbb{F}_q^m$.

Выберем некоторое множество $A = \{\alpha_1, \alpha_2, \dots, \alpha_l\}$ линейно независимых над $\mathbb{F}_q$ элементов $\mathbb{F}_q^m$. Кодирование будет выглядеть следующим образом. Пусть $f = (f_0, f_1, \dots, f_{k-1}) \in \mathbb{F}_{q^m}^k$ – информационное сообщение, которое требуется передать всем получателям. По информационному вектору строится информационный линеаризованный многочлен $f(x) = \sum_{i=0}^{k-1} f_i x^{q^i} \in \mathbb{F}_{q^m}[x]$.

Для полученного многочлена $f(x)$ во всех точках множества A вычисляется его значение: $\beta_i = \mathcal{T}(f(\mathcal{T}^{-1}\alpha_i))$. Образуются пары (α_i, β_i), которые можно рассматривать как элементы $\mathbb{F}_q^{2m}$, принадлежащие объемлющему пространству $W = \langle A \rangle \oplus \mathbb{F}_q^m$ размерности $l + m$. Поскольку множество A состояло из линейно независимых над $\mathbb{F}_q$ элементов, то как элементы пространства $\mathbb{F}_q^{2m}$ множество пар $\{(\alpha_1, \beta_1), (\alpha_2, \beta_2), \dots, (\alpha_l, \beta_l)\}$ является линейно независимым над $\mathbb{F}_q$, и, следовательно, порождает l-мерное пространство V. Следует отметить, что все элементы порожденного подпространства имеют структуру $(a, \mathcal{T}(f(\mathcal{T}^{-1}a)))$. Действительно, в силу линеаризованности полинома, выполняется его основное свойство – линейность относительно младшего поля:

$$\forall x, y \in \mathbb{F}_{q^m} \ \forall a, b \in \mathbb{F}_q \quad f(ax + by) = af(x) + bf(y).$$

При этом любой элемент V представим в виде

$$\left(\sum_{i=1}^{l} c_i\alpha_i \ , \ \sum_{i=1}^{l} c_i T(f(\mathcal{T}^{-1}(\alpha_i)))\right) = \left(\sum_{i=1}^{l} c_i\alpha_i \ , \ \mathcal{T}(\sum_{i=1}^{l} f(\mathcal{T}^{-1}(c_i\alpha_i)))\right),$$

так как $c_i \in \mathbb{F}_q$, то есть сохраняет искомую структуру.

Введем отображение вычисления $ev_A: \mathbb{F}_{q^m}^k \to Gr_l(\mathbb{F}_q^{2m})$, сопоставляющее вектору $f \in \mathbb{F}_{q^m}^k$ -мерное линейное пространство порожденное базисом из пар вида (α_i, β_i). Напомним, что через $Gr_l(\mathrm{K})$ обозначают грассманиан пространства K раз-

мерности l, т.е. множество всех подпространств пространства К указанной размерности. В [8] доказывается, что при $l \geq k$ отображение ev_A является инъективным. Далее везде будем считать, что $l \geq k$.

Образ отображения ev_A называют сетевым подпространственным кодом типа кода Рида-Соломона. Следует отметить, что хотя результатом кодирования является подпространство – элемент грассманиана, при этом реально по сети передается не подпространство, а его базис, то есть элемент пространства Штифеля. Более того, для алгоритмов кодирования и декодирования удобно использовать как раз представление через базис передаваемого подпространства.

На множестве $\mathcal{P}(W)$ вводится метрика и кодовое расстояние кода C:

$$d(A,B) = \dim(A+B) - \dim(A \cup B), \quad D(C) = \min_{X,Y \in C: X \neq Y} d(X,Y).$$

Минимальное кодовое расстояние сетевого РС-кода C определяется по формуле $D(C) = 2(l-k+1)$. Такой код может исправить не более ρ стираний и t ошибок, где

$$\rho + t < D(C)/2 = l - k + 1.$$

Алгоритм 1. Кодирование сетевых кодов типа кода Рида-Соломона.

Вход: информационный вектор $f = (f_0, f_1, \dots, f_{k-1}) \in \mathbb{F}_{q^m}^k$, параметр $l \geq k$, множество линейно независимых над $\mathbb{F}_q$ элементов $\mathbb{F}_q^m$ $A = \{\alpha_1, \alpha_2, \dots, \alpha_l\}$, определяющее код C.

Выход: базис кодового подпространства $V \in C$.

1. Для всех $j = 1, \dots, l$ вычислить

$$\beta_j = \mathcal{T}\left(\sum_{i=0}^{k-1} f_i (\mathcal{T}^{-1}(\alpha_j))^{q^i}\right).$$

2. Вернуть множество линейно независимых векторов

$$\{(\alpha_1, \beta_1), (\alpha_2, \beta_2), \dots, (\alpha_l, \beta_l)\}. \bullet$$

Для построения системы защиты в разделе 3 необходимо построить матричную интерпретацию кодирования. Кодирование РС-кодов содержит два важных действия: вычисление линеаризованного полинома в заданном наборе точек и составление пар вида «(точка, значение полинома)». Вычисление полинома, как и в случае канала, можно представить обычным умножением на матрицу Вандермонда. Кроме того, требуется, чтобы все действия с точкой и значением в ней происходили одновременно. Это можно записать в матричном виде и преобразовать алгоритм кодирования 1:

$$\begin{pmatrix} \alpha_1 & \dots & \alpha_l \\ f(\alpha_1) & \dots & f(\alpha_l) \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ f_0 & f_1 & \dots & f_{k-1} \end{pmatrix} \begin{pmatrix} \alpha_1 & \dots & \alpha_l \\ \alpha_1^q & \dots & \alpha_l^q \\ & \dots & \\ \alpha_1^{q^{k-1}} & \dots & \alpha_l^{q^{k-1}} \end{pmatrix}.$$

Таким образом, кодовая матрица сетевого РС-кода, порожденного множеством $A = \{\alpha_1, \alpha_2, \dots, \alpha_l\}$ будет иметь вид

$$G = \begin{pmatrix} \alpha_1 & \dots & \alpha_l \\ \alpha_1^q & \dots & \alpha_l^q \\ & \dots & \\ \alpha_1^{q^{k-1}} & \dots & \alpha_l^{q^{k-1}} \end{pmatrix}. \quad (1)$$

Алгоритм 2. Матричное кодирование сетевых РС-кодов.

Вход: информационный вектор $f = (f_0, f_1, \dots, f_{k-1}) \in \mathbb{F}_{q^m}^k$, кодовая матрица G, определяющая код C.

Выход: базис кодового подпространства $V \in C$.

1. Построить матрицу

$$F = \begin{pmatrix} 1 & 0 & \dots & 0 \\ f_0 & f_1 & \dots & f_{k-1} \end{pmatrix}$$

2. Вычислить $R = FG$.

3. Вернуть множество столбцов полученной матрицы R, представив их как векторы над младшим полем $\mathbb{F}_q$. •

Опишем алгоритм декодирования из [9]. Алгоритм работает корректно при допущении не более допустимого количества ошибок t и стираний ρ, то есть, как отмечалось ранее, при $\rho + t < l - k + 1$.

Алгоритм 3. Декодирование сетевых кодов типа кода Рида-Соломона.

Вход: порождающая система пространства $U \in Gr_r(\mathbb{F}_q^{2m})$.

Выход: информационный вектор $f \in \mathbb{F}_{q^m}^k$, если произошло не более допустимого количества ошибок и стираний, или ошибка декодирования, иначе.

1. Найти произвольный базис подпространства U: (x_i, y_i), $i = 1, \dots, r$.

2. Определить параметр $\tau = \lfloor (r + k)/2 \rfloor$.

3. При помощи алгоритма интерполяции из [8], найти ненулевой полином $Q(x, y) = Q_x(x) + Q_y(y)$ как сумму двух линеаризованных полиномов $Q_x(x)$ и $Q_y(y)$, для которого все векторы (x_i, y_i), $i = 1, \dots, r$ являются нулями. Если степень хотя бы одного многочлена превышает допустимую, т.е. $\deg Q_x(x) > q^{\tau-1}$ или $\deg Q_y(y) > q^{\tau-k}$, вернуть ошибку декодирования.

4. При помощи алгоритма правого деления линеаризованных полиномов из [9], с. 19, найти полином $f(x)$ из уравнения $Q_y(x) \otimes f(x) + Q_x(x) \equiv 0$, то есть $Q_y\big(f(x)\big) + Q_x(x) \equiv 0$. Если вернулась ошибка, вернуть ошибку декодирования.

5. По коэффициентам найденного полинома $f(x) = \sum_{i=0}^{k-1} f_i x^{q^i}$ найти и вернуть вектор $f = (f_0, f_1, \dots, f_{k-1})$. •

3. Система защиты Мак-Элиса на сетевых РС-кодах. В построенной ниже системе с открытым ключом отправитель обладает конфиденциальной информацией, с помощью общеизвестного открытого ключа зашифровывает информацию и отправляет шифрограмму по случайной линейной сети получателям, владеющим секретным ключом расшифрования. Таким образом, проявляется одно из отличий от криптосистемы Мак-Элиса для канала, где рассматривался случай, когда многим пользователям требовалось передать конфиденциальную информацию серверу, обладающему секретным ключом. В случае сети же наоборот, один отправитель шифрует общеизвестным открытым ключом сообщение, и отправляет его многим получателям, владеющим одним и тем же секретным ключом. На практике такой случай может быть, например, если разведчику требуется передать всем штабам одновременно конфиденциальную информацию.

Впервые криптосистема с открытым ключом было предложена в работе Диффи и Хеллмана [10], а Мак-Элис предложил строить такие криптосистемы на основе помехоустойчивых линейных кодов [11]. Криптосистема Мак-Элиса на базе кодов Рида-Соломона была взломана Сидельниковым [5], однако аналогичная криптосистема на базе кодов Гоппы является не взломанной по настоящее время.

В сетевом случае построим некоторый аналог криптосистемы Мак-Элиса в том смысле, что это по-прежнему будет криптосистема с открытым ключом на базе помехоустойчивого кода, но теперь уже не для канала, а для сети, и на базе сетевого кода. Кодирование сетевых кодов будем рассматривать с точки зрения построенной в разделе 2 его матричной интерпретации.

Как и в случае канала, защита строится от наблюдателя, который может частично или полностью перехватить передаваемое по сети сообщение, и, зная алгоритмы шифрования, расшифрования и открытый ключ, пытается восстановить исходное сообщение. Целью криптосистемы является защитить передаваемую информацию от такого наблюдателя.

В случае криптосистемы Мак-Элиса для канала передачи данных на базе помехоустойчивого (n, k)-кода открытый ключ является $(k \times n)$-матрицей SGP, где G – общеизвестная кодирующая $(k \times n)$-матрица кода, выбранного как раза криптосистемы, S – произвольная невырожденная $(k \times k)$-матрица, P – произвольная перемешивающая $(n \times n)$-матрица. Фактически матрица S не меняет кода, матрица SG будет по-прежнему кодирующей для того же кода. Матрица P перемешивает координаты кода, так как матрицы SG и SGP отличаются лишь перестановкой столбцов.

Распишем основные параметры сетевой криптосистемы.

Секретный ключ: случайная невырожденная $(k \times k)$-матрица S с первой строкой веса 1 над полем $\mathbb{F}_{q^m}$, случайная невырожденная $(l \times l)$-матрица P с элементами из поля $\mathbb{F}_q$.

Открытый ключ: кодирующая $(k \times l)$-матрица G сетевого РС-кода из уравнения (1), $(k \times l)$-матрица $M = SGP$ над полем $\mathbb{F}_{q^m}$.

По поводу генерации ключей системы защиты следует отметить, что матрицы S и P можно генерировать случайным образом над соответствущем полем, а затем проверять, являются ли он невырожденными. Касательно дополнительного условия на вес первой строки матрицы S, можно сначала случайно ее генерировать, затем случайным образом обнулить все элементы первой строки, кроме одного, а уже затее проверять ее невырожденность.

Алгоритм 4. Шифрование.

Вход: информационное сообщение $f = (f_0, f_1, \dots, f_{k-1}) \in \mathbb{F}_{q^m}^k$.

Выход: базис шифрограммы $U \in Gr_r(\mathbb{F}_q^{2m})$.

1. Построить матрицу

$$F = \begin{pmatrix} 1 & 0 & \dots & 0 \\ f_0 & f_1 & \dots & f_{k-1} \end{pmatrix}$$

2. Вычислить $R = FM$.

3. Вернуть набор столбцов полученной матрицы R, представив их как векторы над младшим полем $\mathbb{F}_q$. •

Следует сделать замечание, что в случае, когда заранее известно, что при передаче по сети не будет появляться ошибок и стираний, можно для дополнительной криптостойкости добавить ошибку максимально допустимого для декодера веса δ, то есть на третьем шаге алгоритма шифрования 4 вернуть новый базис, являющийся объединением базиса пространства V с δ штук некоторых векторов.

Алгоритм 5. Расшифрование.

Вход: секретный ключ, порождающая система подпространства U.

Выход: информационное сообщение f длины k или ошибка декодирования.

1. Вычислить базис подпространства U: $\{(x_i, y_i)\}, i = 1, \dots, r$.

2. Найти индекс j ненулевого элемента $s_{1,j}$ первой строки матрицы S.

3. Преобразовать базисные пары по правилу $(x_i, y_i) := ((x_i / s_{1,j})^{q^{m-j+1}}, y_i)$.

4. Отправить полученные на предыдущем шаге алгоритма пары (x_i, y_i) на вход алгоритма декодирования 2. Получить сообщение $\tilde{f}$ или ошибку декодирования.

5. Вычислить $f = \tilde{f} S^{-1}$. Вернуть f. •

Теорема. *Алгоритмы шифрования 4 и расшифрования 5 работают корректно, то есть если было зашифровано некоторое информационное сообщение, и затем передано по сети получателям, то каждый получатель сможет восстановить алгоритмом расшифрования исходное информационное слово, если в полученном слове было допущено не более исправимого кодом количества ошибок и стираний.*

Доказательство. Сначала проследим вклад при шифровании алгоритмом 4 невырожденной матрицы P над младшим полем.

В результате шифрования по сети фактически передается фиксированный базис полученного подпространства. Однако по сути сети, объектом передачи является не фиксированный базис, а подпространство, порожденное этим базисом. Поэтому не имеет значения, какой именно базис подпространства будет передаваться.

Для удобства будем дальше говорить, что множество столбцов $(2 \times l)$-матрицы K над полем $\mathbb{F}_{q^m}$ определяет подпространство, подразумевая, что это подпространство порождено линейно независимой системой, полученной при переводе множества столбцов во множество векторов длины $2m$ над младшим полем $\mathbb{F}_q$.

Шифрование определяется результатом вычисления произведения матриц $R = FSGP$. Матрица P умножается слева на матрицу FSG, и, кроме того, является невырожденной с элементами из младшего поля. Поэтому множество столбцов матрицы FSG определяет то же подпространство, что и множество столбцов матрицы $FSGP$. По сути, подпространство не меняется, еняется лишь представляющий его базис. Более того, она никак не влияет и на вес ошибки при передаче, в отличие от случая обычного канала. Следует отметить, что матрица P не добавляет зашумления шифрограмме, однако является дополнительным зашумляющим средством для секретного ключа.

Далее будем доказывать корректность работы алгоритмов, игнорируя матрицу P.

При подробном изучении, шифрование, уже без матрицы P, будет выглядеть следующим образом:

$$FSG = \begin{pmatrix} 1 & 0 & \dots & 0 \\ f_0 & f_1 & \dots & f_{k-1} \end{pmatrix} \begin{pmatrix} s_{1,1} & \dots & s_{1,k} \\ s_{2,1} & \dots & s_{2,k} \\ & \dots & \\ s_{k,1} & \dots & s_{k,k} \end{pmatrix} \begin{pmatrix} \alpha_1 & \dots & \alpha_l \\ \alpha_1^q & \dots & \alpha_l^q \\ & \dots & \\ \alpha_1^{q^{k-1}} & \dots & \alpha_l^{q^{k-1}} \end{pmatrix} =$$

$$= \begin{pmatrix} s_{1,1} & \dots & s_{1,k} \\ \tilde{f}_0 & \dots & \tilde{f}_{k-1} \end{pmatrix} \begin{pmatrix} \alpha_1 & \dots & \alpha_l \\ \alpha_1^q & \dots & \alpha_l^q \\ & \dots & \\ \alpha_1^{q^{k-1}} & \dots & \alpha_l^{q^{k-1}} \end{pmatrix} = \begin{pmatrix} s_1(\alpha_1) & \dots & s_1(\alpha_l) \\ \tilde{f}(\alpha_1) & \dots & \tilde{f}(\alpha_l) \end{pmatrix}, \qquad (2)$$

где $s_1(\mathrm{x})$ – линеаризованный многочлен, порожденный первой строкой матрицы S, $\tilde{f}(x)$ – линеаризованный многочлен, порожденный коэффициентами вектора fS.

При описании секретного ключа требовалось, чтобы первая строка секретной матрицы S имела единичный вес, поэтому результат шифрования будет иметь следующий вид:

$$\begin{pmatrix} s_{1,j}\alpha_1^{q^{j-1}} & s_{1,j}\alpha_2^{q^{j-1}} & \dots & s_{1,j}\alpha_l^{q^{j-1}} \\ \tilde{f}(\alpha_1) & \tilde{f}(\alpha_2) & \dots & \tilde{f}(\alpha_l) \end{pmatrix},$$

где j – индекс ненулевого элемента первой строки S от 1 до k. Столбцы полученной матрицы будут линейно независимыми как векторы длины $2m$ над полем $\mathbb{F}_q$, то есть действительно будут базисом некоторого подпространства.

При прохождении по сети с векторами полученной матрицы будут совершаться некоторые случайные линейные комбинации над младшим полем, и в результате каждый безошибочно полученный базисный вектор можно представить в виде:

$$\left(\sum_{i=1}^{l} \gamma_i s_{1,j} \alpha_i^{q^{j-1}}, \sum_{i=1}^{l} \gamma_i \tilde{f}(\alpha_i)\right) = \left(s_{1,j} \sum_{i=1}^{l} \gamma_i \alpha_i^{q^{j-1}}, \tilde{f}\left(\sum_{i=1}^{l} \gamma_i \alpha_i\right)\right),$$

где $\gamma_i \in \mathbb{F}_q$ – некоторые неизвестные коэффициенты. В соответствии с алгоритмом расшифрования 5 с данными парами нужно провести преобразования:

$$x_i := (x_i / s_{1,j})^{q^{m-j+1}},$$

$$x_i := \left((s_{1,j} \sum_{i=1}^{l} \gamma_i \alpha_i^{q^{j-1}}) / s_{1,j}\right)^{q^{m-j+1}} = \left(\sum_{i=1}^{l} \gamma_i \alpha_i^{q^{j-1}}\right)^{q^{m-j+1}} =$$

$$= \sum_{i=1}^{l} (\gamma_i)^{q^{m-j+1}} \left(\alpha_i^{q^{j-1}}\right)^{q^{m-j+1}} = \sum_{i=1}^{l} \gamma_i \alpha_i^{q^m} = \sum_{i=1}^{l} \gamma_i \alpha_i.$$

Таким образом, новые корректно полученные пары принимают вид:

$$\left(\sum_{i=1}^{l} \gamma_i \alpha_i, \tilde{f}\left(\sum_{i=1}^{l} \gamma_i \alpha_i\right)\right),$$

то есть имеют структуру пар «(точка, значение в ней)». Аналогично преобразовываются и векторы ошибок, но они продолжают оставаться случайными и неизвестными.

Новые пары отправляются на вход алгоритма декодирования 3, и, если допущено не более допустимого количества ошибок и стираний, декодер возвращает вектор $\tilde{f}$. Умножая на обратную к матрице S получим искомый вектор:

$$\tilde{f} S^{-1} = (fS) S^{-1} = f.$$

Таким образом, пара алгоритмов работает корректно. •

Рассмотрим стойкость криптосистемы от наблюдателя. Для этого сначала построим модель наблюдателя.

Наблюдатель может прослушивать любой фрагмент сети, то есть, в худшем случае, перехватить весь передаваемый базис шифрограммы. В случае, когда наблюдатель перехватил порождающую систему недостаточной размерности, наблюдатель может подбирать перебором недостающие векторы. Однако, будем предполагать, что в силе худший случай, и наблюдатель смог перехватить всю шифрограмму.

Предполагается, что наблюдатель действует в условиях бесконечного времени.

В соответствии с моделью криптосистемы, наблюдателю известен открытый ключ и неизвестен секретный. Таким образом, перед наблюдателем становится две задачи – либо совершать атаку на шифрограмму с целью получить расшифровку конкретной шифрограммы, либо совершать атаку на секретный ключ.

Без знания секретного ключа наблюдатель не сможет преобразовать полученные пары к искомой структуре и воспользоваться декодером. Таким образом, не проходит прямой алгоритм расшифрования и атака на шифрограмму. Атака на ключ предполагает факторизацию общеизвестной матрицы $M = SGP$ на составляющие её матрицы S, G и P при условии, что матрица G известна. Как отмечалось раньше, в случае канала решена подобная задача взлома, когда G – кодирующая матрица кода Рида-Соломона, S – квадратная невырожденная матрица, а P – квадратная перестановочная матрица [5]. Разрешенный случай отличается от рассмотренного в настоящей работе, поскольку здесь кодовая матрица G имеет немного другой вид (по сравнению с матрицей Вандермонда здесь пропущены некоторые строки), а также матрица P имеет более общий вид. Более подробное выяснение стойкости рассматриваемой криптосистемы при атаке на ключ не являлось целью настоящей работы.

4. Симметричная сетевая кодовая система защиты. В системе защиты, рассмотренной в предыдущем пункте, одной из особенностей является то, что матрица секретного ключа P никак не влияет на расшифрование. В случае криптосистемы Мак-Элиса для канала матрица P играет роль перестановки координат шифрограммы. Как отмечалось в теореме о корректности работы алгоритмов 4-5, матрица секретного ключа P изменяет лишь базис зашифрованного подпространства, однако не меняет самого подпространства.

Результатом шифрования является набор линейно независимых векторов длины $2m$ над полем $\mathbb{F}_q$. Если попытаться оставить логику перестановочной матрицы, то можно переставлять координаты шифрограммы уже после перехода к векторам над младшим полем.

Однако в данном случае не удается сохранить логику системы защиты с открытым ключом – необходимо, чтобы и отправитель, и получатели знали секретный ключ, неизвестный всем остальным.

Таким образом, секретный ключ будет по-прежнему содержать матрицы S и P, но теперь добавляется случайная перестановочная $(2m \times 2m)$-матрица P_2 над полем $\mathbb{F}_q$.

Алгоритмы 4–5 изменятся следующим образом. В алгоритме шифрования изменится шаг 3 и добавится шаг 4:

3. Представить набор столбцов полученной матрицы R их как векторы над младшим полем $\mathbb{F}_q$ и записать их последовательно в столбцы $(2m \times l)$-матрицы R_2.

4. Вычислить произведение R_2P_2 и вернуть множество столбцов полученной матрицы.

В алгоритме расшифрования после шага 1 добавится шаг 1.1:

1.1. Полученные векторы базиса последовательно записать в $(2m \times l)$-матрицу R_2. Вычислить произведение $R_2{P_2}^{-1}$ и передать на следующий шаг множество столбцов полученной матрицы.

Однако данный метод имеет ряд достоинств и недостатков. К достоинствам метода можно отнести то, что введение перестановочной матрицы увеличивает криптостойкость шифрограммы. Переход от младшего поля к старшему нельзя записать умножением на матрицу, а значит, полученная система защиты уже не будет системой защиты с открытым ключом, а станет симметричной, что с одной стороны является недостатком. Но при этом с другой стороны, ситуация, когда одному отправителю следует передать получателям зашифрованную известным им обоим секретным ключом информацию, является распространенной на практике. Например, это может быть случай шифрованного цифрового телевидения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2005. – 320 с.
2. *Деундяк В.М., Михайлова Е.А.* Применение матриц Вандермонда при передаче данных по q-ичному каналу со стираниями // Изв. ВУЗов. Северо-Кавказский регион. Естественные науки. – 2012. – № 3. – С. 5-9.
3. *Михайлова Е.А.* О реализации схемы В.Пана защиты информации в канале со стираниями // Математика и её приложения: Журнал Ивановского математического общества. – 2011. – Вып. 1 (8). – С. 75-78.
4. *Шнайер Б.* Прикладная криптография. – М.: ТРИУМФ, 2002. – 816 с.
5. *Сидельников В.М.* Теория кодирования. – М.: Физматлит, 2006. – 324 с.
6. *Габидулин Э.М., Пилипчук Н.И., Колыбельников А.И., Уривский А.В., Владимиров С.М., Григорьев А.А.* Сетевое кодирование // Труды МФТИ. – 2009. – Т. 1, № 2. – С. 3-28.

7. *Alshwede R., Cai N., Li S.-Y. R., Yeung R.W.* Network information flow // IEEE Trans. Inf. Theory. – 2000. – Vol. 46. – P. 1204-1216.
8. *Koetter R., Kschischang F.R.* Coding for errors and erasures in random network coding // IEEE Trans. Inf. Theory. – 2008 – Vol. IT-54, № 8. – P. 3579-3591.
9. *Li S.-Y. R., Yeung R. W., Cai N.* Linear network coding // IEEE Trans. Inf. Theory. – 2003. – Vol. 49. – P. 371-381.
10. *Diffie W., Hellman M.E.* New Directions in Cryptography // IEEE Trans. Inf. Theory. – 1976. – Vol. IT-22, № 6. – P. 644-654.
11. *McEliece R.J.* A Public Key Cryptosystem Based o Algebraic Coding Theory // JPL DSN Progress Rep. – 1978. – Vol. 42-44. – P. 114-116.

Статью рекомендовал к опубликованию к.т.н., доцент Н.С. Могилевская.

Михайлова Екатерина Александровна – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: mikhailovaekaterina@yandex.ru; 344000, г. Ростов-на-Дону, ул. Красноармейская, 196, кв. 8; тел.: 89185879710; кафедра алгебры и дискретной математики; аспирантка.

Mikhailova Ekaterina Aleksandrovna – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: mikhailovaekaterina@yandex.ru; 196, Krasnoarmejskaya street, fl. 8, Rostov-on-Don, 344000, Russia; phone: +79185879710; the department of algebra and discrete mathematics; postgraduate student.

УДК 519.72

В.О. Осипян, Ю.А. Карпенко, А.С. Жук, А.Х. Арутюнян

ДИОФАНТОВЫ ТРУДНОСТИ АТАК НА НЕСТАНДАРТНЫЕ РЮКЗАЧНЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Развитие ассиметричной криптографии началось с появления первой рюкзачной системы защиты информации, когда в 1976 году Ральф Меркель и Мартин Хеллман предложили использовать разные ключи для прямого и обратного преобразования данных при шифровании. На данный момент эта модель, как и многие, основанные на ней были скомпрометированы. Как следствие, авторитет рюкзачных систем занижен. Тем не менее, некоторые из них, до сих пор считаются стойкими, например, модель, предложенная в 1988 году Беном Шором и Рональдом Ривестом. В данной работе сформулирована и решена задача аргументации криптографической стойкости нестандартных рюкзачных систем защиты информации, которые допускают повторное использование элементов рюкзака. Обоснованы диофантовы трудности, возникающие при поиске уязвимостей в указанных системах защиты информации. На основе анализа ранее предложенных рюкзачных моделей выявлены качественные особенности нестандартных рюкзачных систем, повышающие их стойкость к известным атакам.

Рюкзачные системы защиты информации; стойкость алгоритма; криптографическая атака, диофантовы трудности; рюкзачный алгоритм; рюкзачный вектор; исходное сообщение; открытый текст; ключ; шифртекст.

V.O. Osipyan, Yu.A. Karpenko, A.S. Zhuck, A.H. Arutyunyan

DIOPHANTINE DIFFICULTIES OF ATTACKS ON NON-STANDARD KNAPSACKS INFORMATION SECURITY SYSTEMS

Development of the asymmetric cryptography started with the appearance of the first knapsack information protection system, when, in 1976, Ralph Merkel and Martin Hellman proposed to use different keys for forward and reverse mapping data for encryption. Now this model, like many based on are considered to be insecure. As a result the authority of knapsack systems was low.