СХЕМА РАЗДЕЛЕННОЙ ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ НА ОСНОВЕ ДИФФЕРЕНЦИРОВАНИЯ ПОЛИНОМОВ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ НАД ПРОСТЫМИ ПОЛЯМИ ГАЛУА

***Деундяк В.М.*[1] , *Могилевская Н.С.*[2]**

Построена теоретическая схема разделенной передачи конфиденциальных данных, в которой исходные данные на стороне отправителя разделяются на несколько частей и независимо друг от друга передаются по различным линиям связи, а на стороне получателя из принятых частей восстанавливаются исходные данные. Для разделения и восстановления данных используется математический аппарат дифференцирования и интегрирования полиномов m переменных над простыми полями Галуа Fp, а также коды Рида–Маллера второго и первого порядков. Отличительная особенность схемы состоит в том, что ее использование обеспечивает как конфиденциальность, так и помехоустойчивость передаваемых данных. Ключом является набор базисных векторов m–мерного пространства над полем Fp. Определены условия на количество ошибок, при выполнении которых данная схема работает корректно. Приведены оценки размера ключевого пространства схемы и ее избыточности. Описана уязвимость схемы разделенной передачи конфиденциальных данных к атакам на ключ, проводимых на основе однократных и многократных перехватов данных в отдельных линиях связи. Подробно рассмотрена атака на ключ в случае однократного перехвата данных из одной линии связи и оценена ее сложность.

***Ключевые слова**: декомпозиция данных, разделение данных, коды Рида–Маллера, конфиденциальность, помехоустойчивость, полиномы нескольких переменных, параллельные линии связи.*

DOI: 10.21681/2311-3456-2017-5-64-71

1. Введение

В разделенной передаче данных предполагается, что исходные данные на стороне отправителя разделяются на несколько частей, которые независимо друг от друга передаются по различным линиям связи, а на стороне получателя из этих частей восстанавливаются исходные данные. В качестве используемых каналов связи могут выступать как несколько отдельных параллельных каналов связи, так и многоканальная система передачи [1]. Разделенная передача может быть использована как для повышения скорости связи, так и для обеспечения конфиденциальности данных за счет усложнения задачи перехвата. Отметим, что метод декомпозиции данных для обеспечения конфиденциальности используется, например, в криптографических протоколах разделения секретов [2], в методах порогового разделения данных [3, 4], в теории ущербных текстов [5].

Цель работы состоит в создании теоретической схемы разделенной передачи конфиденциальных данных по зашумленным каналам связи на основе использования p-ичных кодов Рида-Маллера и дифференцирования полиномов нескольких переменных. Особенностью предлагаемой схемы декомпозиции данных является то, что она позволяет защищать данные, как от нелегитимного доступа, так и от непреднамеренных ошибок, при этом в обоих случаях используется один и тот же математический аппарат. Отметим, что в работе рассматривается ситуация идеально синхронизированных каналов связи.

2. Дифференциальное исчисление полиномов нескольких переменных и коды Рида-Маллера

В пункте 2.1 этого раздела приведены необходимые сведения [6, 7, 8, 9, 10] и результаты о p-ичных кодах Рида-Маллера и дифференциальном исчислении полиномов нескольких переменных над простыми полями Галуа $\mathbf{F}_p$. В пункте 2.2 доказана теорема, необходимая для обоснования корректности схемы распределенной передачи данных, представленной далее в разделе 3.

2.1. Рассмотрим $\mathbf{F}_p[x_1,...,x_m]$ – кольцо полиномов от m переменных над простым полем $\mathbf{F}_p$. Пусть $\mathbf{F}_p^m$ – m-мерное линейное пространство над $\mathbf{F}_p$. Сумму координат вектора $\overline{\alpha} \in \mathbf{F}_p^m$, как на-

1 Деундяк Владимир Михайлович (ORCID: 0000-0001-8258-2419), кандидат физико-математических наук, доцент, ФГНУ НИИ «Спецвузавтоматика», Институт математики, механики и компьютерных наук Южного федерального университета, г. Ростов-на-Дону, Россия. E-mail: vl.deundyak@gmail.com;

2 Могилевская Надежда Сергеевна (ORCID: 0000-0003-1357-5869), кандидат технических наук, доцент, Донской государственный технический университет, г. Ростов-на-Дону, Россия. E-mail: nadezhda.mogilevskaia@yandex.ru

туральных чисел, обозначим $\rho(\bar{\alpha})$. В векторном пространстве $\mathbf{F}_p^m$ зафиксируем упорядочение

$$\{\bar{\alpha}_1, ..., \bar{\alpha}_n\}\ (\bar{\alpha}_j = (\alpha_{j1}, \alpha_{j2}, ..., \alpha_{jm})\ ), \quad (1)$$

в котором элементы расположены по возрастанию $\rho(\bar{\alpha})$, а при одинаковых значениях $\rho(\bar{\alpha})$ упорядочены лексикографически. В частности, $\bar{\alpha}_1 = \bar{0}$.

Полиномы из $\mathbf{F}_p[x_1,...,x_m]$ будем записывать в каноническом виде

$$f(\bar{x}) = \sum_{\bar{\alpha}\in\mathbf{F}_p^m} f_{\bar{\alpha}}\bar{x}^{\bar{\alpha}},$$

где $\bar{x}^{\bar{\alpha}} = x_1^{\alpha_1}...x_m^{\alpha_m}$, а порядок слагаемых в сумме соответствует (1). Степень монома $\varphi = ax_1^{\gamma_1}...x_m^{\gamma_m} = a\bar{x}^{\bar{\gamma}}$ определяется как $\deg(\varphi) = \rho(\bar{\gamma})$, а степень $\deg(f)$ полинома f определяется как максимальная степень его ненулевых мономов.

Напомним в удобном виде необходимые сведения о кодах Рида-Маллера (РМ-кодах) над простыми полями $\mathbf{F}_p$ [8, 9]. Линейное пространство полиномов из $\mathbf{F}_p[x_1,...,x_m]$ степени не выше r обозначим $\mathbf{F}_p^{(r)}[x_1,...,x_m]$. Элементы $\mathbf{F}_p^{(r)}[x_1,...,x_m]$ назовем информационными полиномами РМ-кода $RM_p(r,m)$, где $m \ge r \ge 0$, $m \ge 2$; будем записывать их как сумму однородных полиномов степеней от нуля до r:

$$f(\bar{x}) = \sum_{\rho(\bar{\alpha})\le r} a_{\bar{\alpha}}\bar{x}^{\bar{\alpha}} = a_{\bar{0}}\bar{x}^{\bar{0}} + \sum_{\rho(\bar{\alpha})=1} a_{\bar{\alpha}}\bar{x}^{\bar{\alpha}} + ... + \sum_{\rho(\bar{\alpha})=r} a_{\bar{\alpha}}\bar{x}^{\bar{\alpha}}. \quad (2)$$

Вектор $\bar{f}$, составленный из коэффициентов информационного полинома $f(x_1,...,x_m)$, называется информационным вектором, и для нумерации его координат используется упорядочение (1). Кодировать информационный полином $f(\bar{x}) \in \mathbf{F}_p^{(r)}[x_1,...,x_m]$ будем путем вычисления его значений в точках упорядоченного пространства $\mathbf{F}_p^m$:

$$C(f) = (f(\bar{\alpha}_1)\ ...,f(\bar{\alpha}_n)\ ). \quad (3)$$

и тем самым определим оператор кодирования C: $\mathbf{F}_p^{(r)}[x_1,...,x_m] \to \mathbf{F}_p^n$; p-ичный РМ-код с параметрами r, m, определяется следующим образом:

$$RM_p(r,m) = \{(f(\bar{\alpha}_1),...,f(\bar{\alpha}_n))\,|\,f(\bar{x}) \in$$

$$\in \mathbf{F}_p[x_1,...,x_m], \deg(f) \le r\} \subset \mathbf{F}_p^n.$$

Коды $RM_p(r,m)$ образуют семейство линейных блочных $[n,k,d]_p$-кодов, длина n и размерность k которых определяются по формулам

$$n = p^m,\ \ k = \sum_{i=0}^{r}\sum_{j=0}^{\lfloor i/p\rfloor}(-1)^j C_m^j\, C_{i-\dot{p}+m-1}^{m-1}, \quad (4)$$

где $\lfloor\ \rfloor$ – округление до меньшего целого, а минимальное кодовое расстояние d удобно вычислять, используя параметры дуального кода. Кодом, дуальным к $RM_p(r,m)$, является код $RM_p(r^\perp,m)$, где $r^\perp = m(p-1)-r-1$. Пусть ρ – остаток от деления $r^\perp+1$ на $p-1$: $r^\perp+1 = \sigma(p-1)+\rho$, где $\rho < p-1$ тогда параметр d кода $RM_p(r,m)$ задается выражением $d = (\rho+1)p^\sigma$. Отметим, что $d = 2^{m-r}$ при $p = 2$. Параметр r называется порядком кода. Декодеры $[n,k,d]_p$-кода гарантировано исправляют $\lfloor(d-1)/2\rfloor$ ошибок в одном кодовом слове.

Производной полинома $f \in \mathbf{F}_p^{(r)}[x_1,...,x_m]$ по направлению $\bar{b} \in \mathbf{F}_p^m$ называется результат действия оператора дифференцирования:

$$(D_{\bar{b}}f)(\bar{x}) = f_{\bar{b}}(\bar{x}) - f(\bar{x}),\ \ \bar{x} \in \mathbf{F}_p^m, \quad (5)$$

где $f_{\bar{b}}(\bar{x}) = f(\bar{x}+\bar{b})$. Легко показать, что $D_{\bar{b}}f \in \mathbf{F}_p^{(r-1)}[x_1,...,x_m]$, а оператор

$$D_{\bar{b}}f : \mathbf{F}_p^{(r)}[x_1,...,x_m] \to \mathbf{F}_p^{(r-1)}[x_1,...,x_m] \quad (6)$$

является линейным. Из (3) и (6) вытекает: если $f \in \mathbf{F}_p^{(r)}[x_1,...,x_m]$, $\bar{b} \in \mathbf{F}_p^m$, то

$$C(f) \in RM_p(r,m),\ C(D_{\bar{b}}f) \in RM_p(r-1,m). \quad (7)$$

Введем аналог оператора дифференцирования $D_{\bar{b}}$ (см.(6)) для пространства $\mathbf{F}_\mathrm{p}^\mathrm{n}$, где $n = p^m$. Координаты векторов из $\mathbf{F}_\mathrm{p}^\mathrm{n}$ будем нумеровать векторами из $\mathbf{F}_\mathrm{p}^\mathrm{m}$ (см.(1)). Рассмотрим оператор сдвига $\tau_{\bar{b}} : \mathbf{F}_\mathrm{p}^\mathrm{n} \to \mathbf{F}_\mathrm{p}^\mathrm{n}$, действующий по формуле

$$\tau_{\bar{b}}(\bar{a}) = (a_{\bar{\alpha}_1+\bar{b}},...,a_{\bar{\alpha}_n+\bar{b}})$$

где $\bar{a} = (a_{\bar{\alpha}_1},...,a_{\bar{\alpha}_n}) \in \mathbf{F}_\mathrm{p}^\mathrm{n}$, $\bar{b} = (b_1,...,b_m) \in \mathbf{F}_\mathrm{p}^\mathrm{m}$. Отметим, что оператор сдвига $\tau_{\bar{b}}$ является перемешивающим биективным отображением. Оператор $\Delta_{\bar{b}} : \mathbf{F}_\mathrm{p}^\mathrm{n} \to \mathbf{F}_\mathrm{p}^\mathrm{n}$, являющийся аналогом $D_{\bar{b}}$, определим формулой:

$$\Delta_{\bar{b}}(\bar{a}) = \tau_{\bar{b}}(\bar{a}) - \bar{a},\ \bar{a} = (a_{\bar{\alpha}_1},...,a_{\bar{\alpha}_n}) \in \mathbf{F}_\mathrm{p}^\mathrm{n}.$$

Будем называть $\Delta_{\bar{b}}(\bar{a})$ производным вектором вектора $\bar{a}$ по направлению $\bar{b}$.

Лемма 1. Рассмотрим $f \in \mathbf{F}_2^{(2)}[x_1,x_2,..,x_m]$, вектор $\bar{b} = (b_1,...,b_m) \in \mathbf{F}_\mathrm{p}^\mathrm{m}$, разностные операторы $\Delta_{\bar{b}}$, $D_{\bar{b}}$ и оператор кодирования C. Тогда

$$\tau_{\bar{b}}(C(f)) = C(f_{\bar{b}}),\ C(D_{\bar{b}}f) = \Delta_{\bar{b}}(C(f)).$$

Доказательство проводится прямыми выкладками и для $p = 3$ имеется в [9].

2.2 Далее понадобится следующая вспомогательная лемма.

Лемма 2. Пусть $f(\bar{x}) \in \mathbf{F}_p^{(2)}[x_1,...,x_m]$ – информационный полином кода $RM_p(2,m)$ в каноническом виде (2), $\bar{b} = (b_1,...,b_m) \in \mathbf{F}_p^m$, p – простое. Тогда

$$f(\bar{x}) = f_{00...00} + \bar{x}\left(f_{10...00}, f_{01...00},..., f_{00...01}\right)^T + \bar{x}A\bar{x}^T,\ , \quad (8)$$

и при $p > 2$

$$(D_{\bar{b}} f)(\bar{x}) = 2\bar{x}A\bar{b}^T + f(\bar{b}) - f_{00\ldots00}, \quad (9)$$

$$A = \begin{pmatrix} f_{200..00} & f_{110..00}/2 & f_{101..00}/2 & \cdots & f_{100..10}/2 & f_{100..01}/2 \\ f_{110..00}/2 & f_{020..00} & f_{011..00}/2 & \cdots & f_{010..10}/2 & f_{010..01}/2 \\ f_{101..00}/2 & f_{011..00}/2 & f_{002..00} & \cdots & f_{001..10}/2 & f_{001..01}/2 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \cdots \\ f_{100..10}/2 & f_{010..10}/2 & f_{001..10}/2 & \cdots & f_{000..20} & f_{000..11}/2 \\ f_{100..01}/2 & f_{010..01}/2 & f_{001..01}/2 & \cdots & f_{000..11}/2 & f_{000..02} \end{pmatrix},$$

а при $p = 2$

$$(D_{\bar{b}} f)(\bar{x}) = \bar{x}(A + A^T)\bar{b}^T + f(\bar{b}) - f_{00\ldots00}, \quad (10)$$

$$A = \begin{pmatrix} 0 & f_{110..00} & f_{101..00} & \cdots & f_{100..10} & f_{100..01} \\ 0 & 0 & f_{011..00} & \cdots & f_{010..10} & f_{010..01} \\ 0 & 0 & 0 & \cdots & f_{001..10} & f_{001..01} \\ 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & f_{000..11} \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Доказательство в случае $p = 2$ вытекает из [6, с. 139], а при $p > 2$ – из [7]. •

Докажем теорему, которая определяет способ восстановления полинома из $\mathbf{F}_p^{(2)}[x_1, x_2, .., x_m]$ по набору его производных, вычисленных в базисных направлениях, с точностью до постоянного слагаемого.

Теорема 1. Пусть p – простое, $\beta = \{\bar{b}_i = (b_1^i, b_2^i, \ldots, b_m^i) \in \mathbf{F}_p^m\}_{i=1,\ldots,m}$ – некоторый базис пространства $\mathbf{F}_p^m$. Рассмотрим полином $f \in \mathbf{F}_p^{(2)}[x_1, x_2, .., x_m]$ в виде (8):

$$f(\bar{x}) = f_{00\ldots00} + \bar{x}\left(f_{10\ldots00}, f_{01\ldots00}, \ldots, f_{00\ldots01}\right)^T + \bar{x}A\bar{x}^T.$$

Пусть

$$\left\{(D_{\bar{b}_i} f)(\bar{x}) = \alpha_1^i x_1 + \alpha_2^i x_2 + \ldots + \alpha_m^i x_m + \alpha_0^i\right\}_{i=1,\ldots,m} \subset$$

$$\subset \mathbf{F}_p^{(1)}[x_1, x_2, \ldots, x_m]. \quad (11)$$

Рассмотрим матрицы

$$B = (b_j^i)_{i,j=\overline{1,m}} = \begin{pmatrix} b_1^1 & b_1^2 & \cdots & b_1^m \\ b_2^1 & b_2^2 & \cdots & b_2^m \\ \vdots & \vdots & \ddots & \vdots \\ b_m^1 & b_m^2 & \cdots & b_m^m \end{pmatrix},$$

$$\Omega = (\alpha_j^i)_{i,j=\overline{1,m}} = \begin{pmatrix} \alpha_1^1 & \alpha_1^2 & \ldots & \alpha_1^m \\ \alpha_2^1 & \alpha_2^2 & \ldots & \alpha_2^m \\ \vdots & \ldots & \ddots & \vdots \\ \alpha_m^1 & \alpha_m^2 & \cdots & \alpha_m^m \end{pmatrix}.$$

Тогда, если $p > 2$, то

$$A = \tfrac{1}{2}\Omega B^{-1}, \quad (12)$$

если $p = 2$, то

$$A + A^T = \Omega B^{-1}, \quad (13)$$

а матрица A восстанавливается по $A + A^T$ обнулением элементов, расположенных ниже главной диагонали; для любого p

$$\left(f_{10\ldots00}, f_{01\ldots00}, \ldots, f_{00\ldots01}\right)^T =$$

$$= \left(\alpha_0^1 - b_1 A b_1^T, \alpha_0^2 - b_2 A b_2^T, \ldots, \alpha_0^m - b_m A b_m^T\right)B^{-1} \quad (14)$$

Доказательство. Для произвольных векторов $\bar{a}, \bar{b} \in F_p^m$ и $(m \times m)$-матрицы D над полем F_p имеет место равенство:

$$\bar{a}D\bar{b}^T = \bar{b}D^T\bar{a}^T.$$

Поэтому из формул (5), (8) и симметричности матрицы A вытекает:

$$(D_{\bar{b}} f)(\bar{x}) = f(\bar{x} + \bar{b}) - f(\bar{x}) =$$

$$= \bar{b}\left(f_{10\ldots00}, f_{01\ldots00}, \ldots, f_{00\ldots01}\right)^T + 2\bar{x}A\bar{b}^T + \bar{b}A\bar{b}^T.$$

Отсюда и из (9), (11) получаем:

$$\forall\ i = 1, \ldots, m: 2A\bar{b}_i^T = (\alpha_1^i, \alpha_2^i, \ldots, \alpha_m^i)^T, \quad f(\bar{b}_i) - f_{00\ldots00} = \alpha_0^i. \quad (15)$$

Тогда $2AB = \mathrm{Y}$. Следовательно, формула (12) верна.

Из (10) и выражения (11) для $\left(D_{\bar{b}_i} f\right)(\bar{x})$ получаем:

$$\forall\ i = 1, \ldots, m: (A + A^T)\bar{b}_i^T = (\alpha_1^i, \alpha_2^i, \ldots, \alpha_m^i)^T, \quad f(\bar{b}_i) - f_{00\ldots00} = \alpha_0^i. \quad (16)$$

Тогда

$$(A + A^T)B = \Omega,$$

т.е. формула (13) верна. Из леммы 2 вытекает, что матрица A верхнетреугольная с нулевой диагональю, следовательно, матрица A^T нижнетреугольная с нулевой диагональю, таким образом, действительно матрица A восстанавливается из суммы $(A + A^T)$ обнулением элементов, лежащих ниже главной диагонали.

Из (8) следует, что для любого $\bar{b} \in \mathbf{F}_p^m$:

$$f(\bar{b}) - f_{00\ldots00} = \bar{b}\left(f_{10\ldots00}, f_{01\ldots00}, \ldots, f_{00\ldots01}\right)^T + \bar{b}A\bar{b}^T.$$

Возьмем в качестве $\bar{b}$ векторы $\bar{b}_i \in \beta$ и воспользуемся равенством $f(\bar{b}_i) - f_{00\ldots00} = \alpha_0^i$ из (15), (16). Тогда

$$\forall\ i = 1, \ldots, m: \alpha_0^i - \bar{b}_i A\bar{b}_i^T = \bar{b}_i\left(f_{10\ldots00}, f_{01\ldots00}, \ldots, f_{00\ldots01}\right)^T.$$

Отсюда вытекает справедливость (14). •

3. Схема разделенной передачи конфиденциальных данных на основе дифференциального исчисления полиномов

В предлагаемой схеме для разделения и сборки данных используются коды Рида-Маллера $RM_p(1,m)$, $RM_p(2,m)$, заданные над простым полем Галуа $\mathbf{F}_p$. Отметим, что эти коды давно и успешно используются в различных задачах защиты информации [6, 10, 11]. Параметрами схемы являют-

ся p и m. На рисунке 1 представлена подготовка исходного сообщения для разделенной передачи. Источник сообщений (ИС) выдает информационный вектор $\overline{w} \in \mathbf{F}_p^k$, где k – размерность $RM_p(2,m)$. Этот вектор поступает в блок разделения сообщений, включающий в себя кодер кода $RM_p(2,m)$ и делитель сообщений. В кодере вектору $\overline{w}$ сопоставляется информационный полином $w = w(\overline{x})$, который кодируется с использованием оператора (3), и на выходе кодера формируется вектор $C(w) \in \mathbf{F}_p^n$, где n – длина кода $RM_p(2,m)$. На вход делителя сообщений поступают вектор $C(w)$ и упорядоченный набор базисных векторов

$$\beta = \{\overline{b}_i = (b_1^i, b_2^i, ..., b_m^i) \in \mathbf{F}_p^m\}_{i=1,...,m}, \quad (17)$$

который является секретным ключом рассматриваемой схемы. Далее в делителе сообщений с помощью ключа β из кодового вектора $C(w) \in \mathrm{RM_p(2,m)}$ формируются m различных производных векторов

$$\Delta_{\overline{b}_i}(C(w)) = C(D_{\overline{b}_i}(w)) (\in RM_p(1,m) \subset \mathbf{F}_p^n), \ i = \overline{1,m},$$

(см. лемму 1). Затем для каждого вектора $C(D_{\overline{b}_i}(w))$, выполняется конкатенация с первым коэффициентом $f_{00..00} := w(\overline{0})$ кодового вектора $C(w)$:

$$\overline{S}_i = C(D_{\overline{b}_i}(w)) \,||\, f_{00..00} \in \mathbf{F}_p^{n+1}. \quad (18)$$

Далее векторы $\overline{S}_i \in \mathbf{F}_p^{n+1}$, $i = \overline{1,m}$, поступают на вход m различных линий связи.

Очевидно, что во время прохождения по линиям связи векторы $\overline{S}_i$, $i = \overline{1,m}$, могут быть искажены, и из канала связи будут получены векторы $\overline{S}_i'$:

$$\overline{S}_i' = (C(D_{\overline{b}_i}(w)))' \,||\, f'_{00..00} \in \mathbf{F}_p^{n+1}, \ i = \overline{1,m}. \quad (19)$$

где $(C(D_{\overline{b}_i}(w)))'$ – возможно искаженный вектор $C(D_{\overline{b}_i}(w))$, а скаляр $f'_{00..00}$ – возможно искаженное значение $f_{00..00}$. Скаляр $f'_{00..00}$, соответствующий $\overline{S}_i'$, для удобства обозначим $f'_{00..00,i}$.

На рисунке 2 представлена схема восстановления исходного сообщения из m различных сообщений, полученных из каналов связи. Блок восстановления исходного сообщения содержит m декодеров кода $RM_p(1,m)$ и один декодер кода $RM_p(0,m)$, фактически совпадающего с $[m,1,m]_p$ -кодом повторения [10, 12], а также сумматор сообщений. В этом блоке из каждого вектора $\overline{S}_i'$ выделяется две компоненты: $(C(D_{\overline{b}_i}(w)))' \in \mathbf{F}_p^n$ и $f'_{00..00,i}$, $i = \overline{1,m}$. Векторы $(C(D_{\overline{b}_i}(w)))'$ направляются в декодеры кода $RM_p(1,m)$. Отметим, что декодеры могут быть использованы произвольные, например, из работ [13, 14, 15]. На выходе рассматриваемых декодеров формируются полиномы $D'_{\overline{b}_i}(w) \subset \mathbf{F}_p^{(1)}[x_1, x_2, .., x_m]$, $i = 1,...,m$. Из коэффициентов $f'_{00..00,i}$ формируется вектор $(f'_{00..00,1}, f'_{00..00,2}, ..., f'_{00..00,m})$ и подается на вход декодера $RM_p(0,m)$, на выходе которого формируется скаляр $f''_{00..00}$. Затем на вход сумматора сообщений подаются полиномы $D'_{\overline{b}_i}(w) \subset \mathbf{F}_p^{(1)}[x_1, x_2, .., x_m]$,

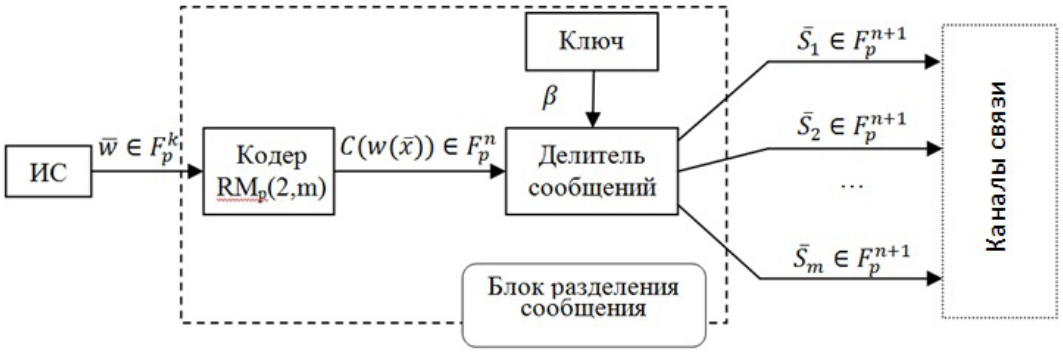

Рис. 1. *Схема разделения сообщений* $C(w)$

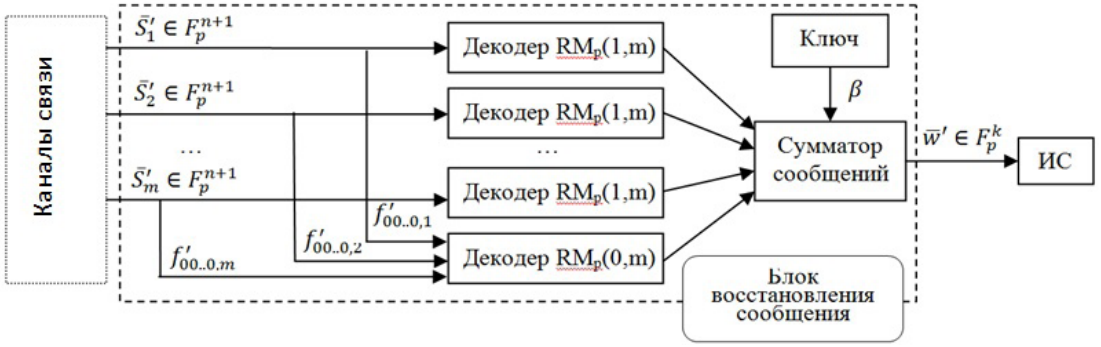

Рис. 2. *Схема восстановления переданного сообщения*

$i=\overline{1,m}$, скаляр $f''_{00..00}$ и ключ β (см. (17)). В сумматоре сообщений формируется полином $f(\bar{x})$, у которого $f_{00..00}$=0, с использованием формул (13) и (14) в случае использования поля мощности два и формул (12) и (14) в случае использование полей другой мощности. Из полинома $f(\bar{x})$ и скаляра $f''_{00..00}$ формируется полином $w'(\bar{x})=f(\bar{x})+f''_{00..00}$, который, как будет ниже доказано в теореме 2, в случае ограниченного числа ошибок совпадает с искомым информационным полиномом $w(\bar{x})\in \mathbf{F}_p^{(2)}[x_1,x_2,..,x_m]$ кода $RM_p(2,m)$. Получателю сообщений поступает информационный вектор $\bar{w}'\in \mathbf{F}_p^k$, соответствующий полиному $w'(\bar{x})$.

Сформулируем связанные с корректирующей способностью кодов Рида-Маллера условия, при выполнении которых предложенная схема корректна.

Теорема 2. Рассмотрим схему разделения сообщений с параметрами p и m. Предположим, что на вход блока разделения сообщения подается информационный вектор $\bar{w}\in \mathbf{F}_p^k$, с выхода этого блока в каждый i-тый канал, $i=1,...,m$, поступает вектор $\bar{S}_i=C(D_{\bar{b}_i}(w))\,||\,f_{00..00}\in \mathbf{F}_p^{n+1}$ (см.(18)), где $f_{00..00}=w(\bar{0})$, а на выходе из этих каналов принимаются векторы $\bar{S}_i'=(C(D_{\bar{b}_i}(w)))'||\,f'_{00..00}\in \mathbf{F}_p^{n+1}$, $i=1,...,m$ (см.(19)). Тогда вектор, полученный на выходе блока восстановления сообщения, совпадет с вектором $\bar{w}$, если выполняются следующие условия:

1) $\forall i=\overline{1,m}:\ d_H(C(D_{\bar{b}_i}(w)),(C(D_{\bar{b}_i}(w)))')\le\lfloor(d_1-1)/2\rfloor$,

где $d_H(\bar{x},\bar{y})$ – расстояние Хемминга между векторами $\bar{x},\bar{y}$, d_1 – минимальное кодовое расстояние кода $RM_p(1,m)$;

2) вектор $(f'_{00..00,1},f'_{00..00,2},...,f'_{00..00,m})$, сформированный в блоке восстановления сообщений, содержит менее $m/2$ координат, отличных от значения $f_{00..00}=w(\bar{0})$.

Доказательство. Часть $C(D_{\bar{b}_i}(w)$ вектора $\bar{S}_i$ является кодовым словом $[n,k_1,d_1]_p$-кода $RM_p(1,m)$ (см.(7), (18)). Параметрами этого кода гарантируется исправление $\lfloor(d_1-1)/2\rfloor$ ошибок в кодовом слове. Следовательно, выполнение первого условия теоремы обеспечивает восстановление любым декодером кода $RM_p(1,m)$ из вектора $(C(D_{\bar{b}_i}(w)))'$ вектора $C(D_{\bar{b}_i}(w)$ и, следовательно, связанного с ним полинома $D_{\bar{b}_i}(w)$.

В блоке восстановления сообщений из координат $f'_{00..00,i}$ векторов $\bar{S}_i'$ формируется вектор $(f'_{00..00,1},f'_{00..00,2},...,f'_{00..00,m})$, являющийся искаженным кодовым словом $[m,1,m]_p$-кода $RM_p(0,m)$, который подается на соответствующий мажоритарный декодер. Параметрами кода $RM_p(0,m)$ гарантируется восстановление значения $f_{00..00}$, если менее, чем $m/2$ координат вектора $(f'_{00..00,1},f'_{00..00,2},...,f'_{00..00,m})$ отличаются от $f_{00..00}$.

Таким образом, условия, наложенные на качество используемых каналов связи, позволяют декодерам в блоке восстановления сообщений (см. рис.2) полностью восстановить все производные $D_{\bar{b}_i}(w)$, $i=\overline{1,m}$ информационного полинома w, а также коэффициент $f_{00..00}=w(\bar{0})$. Корректность восстановления сумматором сообщений исходного полинома w, а, следовательно, и вектора $\bar{w}$, вытекает из теоремы 1. •

Отметим, что в схеме распределенной передачи используются коды Рида-Маллера как первого, так и второго порядков, однако декодеры применяются только для кодов первого порядка и кодов повторения.

Замечание 1. В случае, когда в используемых каналах связи произошло ошибок больше, чем могут исправить декодеры, восстановление информационного вектора не гарантируется. Признаком неверного декодирования в блоке восстановления сообщения является несимметричность матриц A из (12) или $(A+A^T)$ из (13). В этом случае возможно проведение искусственной симметризации матриц. Подобный прием использован в конструкциях декодеров РМ-кодов для поля F_2 в [10, 15], а для поля F_3 в [9, 16]. Вопрос о качестве работы рассматриваемой схемы передачи данных в общем случае требует дополнительного исследования, например, с помощью имитационного моделирования (см., например, [11], глава 4).

Замечание 2. Легко видеть, что объем передаваемых данных увеличивается по сравнению с исходным сообщением в $(n+1)m/k$ раз, но при этом возрастает помехоустойчивость и обеспечивается конфиденциальность. В схеме с параметрами $p=2$ и $m=4$, длина информационного вектора k=11, длина кодового вектора n=16, т.о. по 4 линиям связи передаются векторы длины 17 (см. (4), (18)). Следовательно, объем передаваемых данных увеличивается примерно в 6 раз. При этом декодеры кода $RM_2(1,4)$, используемые на стороне получателя могут исправить не менее трех ошибок в каждом векторе $\bar{S}_i$, $i=1,...,4$. В случае, когда бы разделенная передача не использовалась и в канал связи сразу бы передавался кодовый вектор кода $RM_2(2,4)$, сформированный в блоке разделения сообщений, то объем передаваемых данных увеличился бы в 16/11≈1,45 раз, но используемые декодеры смогли бы исправить

только одну ошибку в принятом векторе. В случае схемы с параметрами $p=3$ и $m=2$: $k=6$, $n=9$, по 2 каналам связи передаются векторы длины 10, объем данных увеличивается примерно в 3,33 раз, при этом, код $RM_3(1,2)$ гарантирует исправление двух ошибок в кодовом слове, а код $RM_3(2,2)$, используемый в блоке разделения сообщений – только одной ошибки, увеличивая при этом длину исходного сообщения в 1,5 раза.

Замечание 3. Мощность N ключевого пространства в случае использования схемы разделенной передачи с параметрами p и m совпадает с количеством всевозможных упорядоченных ключевых наборов β вида (17):

$$N = m! \prod_{i=0}^{m-1} (p^m - p^i). \quad (20)$$

Для сравнения стандарт шифрования ГОСТ 28147-89 предлагает использовать ключ длиной 256 бит, т.е. общее число ключей 2^{256}. В разработанной схеме схожий объем ключевого пространства достигается в двоичном случае при m=15. В этом случае, N»2.04×10^{79}» 2^{263}.

4. Возможные атаки на ключ

Рассмотрим схему разделенной передачи с параметрами p и m, в которой качество линий связи таково, что для легальных пользователей выполняются условия корректности работы, сформулированные в теореме 2. Будем предполагать, что отправителем передается информационный полином $f(\bar{x})$ в виде (8), а за системой следит нелегальный наблюдатель, цель которого восстановить ключ β. Предположим, что наблюдатель способен определять начало и конец векторов $\bar{S}_i' = (C(D_{\bar{b}_i}(w)))' \| f'_{00..00} \in \mathbf{F}_p^{n+1}$, перехваченных из линий связи, и знает упорядочение (1).

Рассмотрим атаку на одну фиксированную линию связи при однократном перехвате, т.е. ситуацию, когда нелегальному наблюдателю удается получить вектор $\bar{S}_i'$ из одной линии связи. Пусть $a(\bar{x}) = a_0 + <\bar{x}, \bar{u}>$ – результат декодирования наблюдателем вектора $(C(D_{\bar{b}_i}(w)))'$. Возникает задача восстановления по вектору $\bar{a} = (a_0 \mid \bar{u})$ полинома $f(\bar{x})$ с k коэффициентами и вектора $\bar{b} = \bar{b}_i (\in \mathbf{F}_p^m)$ для которых $D_{\bar{b}}(f) = a(\bar{x})$. Для поиска таких $\bar{b}$ и $f(\bar{x})$ методом полного перебора при $p > 2$ необходимо рассмотреть $p^m p^k = p^{2m+\frac{m(m+1)}{2}+1}$ вариантов пар $\bar{b}$ и $f(\bar{x})$. Перебор можно уменьшить, если учитывать, что в силу (9) равенство $D_{\bar{b}}(f) = a(\bar{x})$ имеет вид

$$2\bar{x}A\bar{b}^T + f(\bar{b}) - f_{00...00} = a_0 + <\bar{x}, \bar{u}>.$$

В итоге получаем систему из $m+1$ уравнений с $m + \frac{m(m+1)}{2} + 1$ неизвестными:

$$\begin{cases} f(\bar{b}) - f_{00..00} = a_0, \\ 2A\bar{b}^T = \bar{u}, \end{cases} \quad (21)$$

Поэтому можно снизить число переборов до $p^{m+\frac{m(m+1)}{2}}$, предварительно применяя к системе (21) метод Гаусса, вычислительная сложность которого $O((m+1)^3)$. Таким образом, в результате атаки на одну фиксированную линию связи при однократном перехвате, злоумышленник с вычислительной сложностью $O((m+1)^3)$ может получить список из $p^{m+\frac{m(m+1)}{2}}$ подходящих пар $f(\bar{x})$ и $\bar{b}$.

Кроме рассмотренной атаки возможны и другие атаки. Например, атака на одну фиксированную линию связи при повторном (кратном) перехвате, или атака на две и более фиксированные линии связи при одновременном перехвате.

Выводы

В работе построена новая теоретическая схема разделенной передачи конфиденциальных данных, основанная на использовании РМ-кодов. Обоснованы условия корректности ее работы, приведены оценки избыточности и размера ключевого пространства. Схема применима к данным, представленным простыми полями Галуа, и обеспечивает конфиденциальность и помехоустойчивость передачи. Конфиденциальность поддерживается не только закрытостью ключа, но и декомпозицией данных, т.к. перехват из нескольких линий связи затруднительнее для наблюдателя, чем нелегитимное получение данных из одной линии связи. В дальнейшем представляется полезным рассмотреть возможность переноса схемы разделенной передачи на случай произвольных РМ-кодов, а также исследовать устойчивость схемы к общим атакам.

Рецензент: *Косолапов Юрий Владимирович, кандидат технических наук, доцент кафедры Алгебры и дискретной математики Института математики, механики и компьютерных наук Южного федерального университета; заместитель начальника отдела информационной безопасности Департамента безопасности макрорегионального филиала «ЮГ» открытого акционерного общества междугородной и международной электрической связи «РОСТЕЛЕКОМ», г. Краснодар, Россия. E-mail: itaim@mail.ru*

Литература

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение, 2-е издание. : Пер. с англ. – М.: Издательский дом «Вильямс», 2016. 1104 с.
2. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Издательский центр «Академия», 2009. 272 с.
3. Могилевская Н.С., Кульбикаян Р.В., Журавлев Л. А. Пороговое разделение файлов на основе битовых масок: идея и возможное применение // Вестник Донского гос. тех. ун-та, 2011. Т.11. № 10. С. 1749-1755.
4. Тормасов А.Г., Хасин М.А., Пахомов Ю.И. Обеспечение отказоустойчивости в распределенных средах // Программирование. 2001. Т.27. № 5. С. 26.
5. Мищенко В.А., Виланский Ю.В. Ущербные тексты и многоканальная криптография. - Минск: Энциклопедикс, 2007. 292 с.
6. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. 470 с.
7. Деундяк В. М., Кнутова А. В. Интегрируемость систем полиномов нескольких переменных первой и второй степени над простыми полями Галуа // Известия ВУЗов. Северо-Кавказский регион. Естественные науки. 2016. №2. С. 41–46.
8. Pellikaan R., Wu X.-W. List decoding of q-ary Reed-Muller Codes // IEEE Trans. On Information Theory. 2004. Vol. 50 (3). P. 679-682.
9. Деундяк В. М. , Могилевская Н. С. Об условиях корректности декодера мягких решений троичных кодов Рида-Маллера второго порядка. Владикавказский математический журнал. 2016, Т. 18. Вып. 4. С.23-33.
10. Сидельников В.М. Теория кодирования. – М.: ФИЗМАТЛИТ, 2008. 324 с.
11. Гордеев Э.Н., Леонтьев В.К., Медведев Н.В. О свойствах булевых полиномов, актуальных для криптосистем // Вопросы кибербезопасности. 2017. №3 (21). С.63-69.
12. Деундяк В.М., Маевский А.Э., Могилевская Н.С. Методы помехоустойчивой защиты данных. Ростов-на-Дону: Изд-во ЮФУ, 2014. – 309 с.
13. Лицын С. Н., Шеховцов О. И. Быстрый алгоритм декодирования кодов Рида-Маллера первого порядка // Пробл. передачи информ., 1983. 19:2. С. 3–7.
14. Зяблов В.В., Портной С. Л. Быстрое декодирование кодов Рида–Маллера по максимуму правдоподобия // Пробл. передачи информ., 1991. 27:4. С. 39–50.
15. Loidreau P., Sakkour B. Modified version of Sidel'nikov-Pershakov decoding algorithm for binary second order Reed-Muller codes // Ninth International Workshop on Algebraic and Combinatorial Coding theory, ACCT-9., Kranevo, 2004. P.266-271.
16. Деундяк В.М., Могилевская Н.С. Модель троичного канала передачи данных с использованием декодера мягких решений кодов Рида-Маллера второго порядка // Известия вузов. Северо-Кавказский регион. Технические науки, 2015. № 1. С. 3–10.

THE CONFIDENTIAL DATA DIVIDED TRANSMISSION SCHEME BASED ON DIFFERENTIAL CALCULUS OF POLYNOMIALS IN SEVERAL VARIABLES OVER PRIME GALOIS FIELDS

Deundyak V.[3], Mogilevskaya N.[4]

Abstract. *The paper presents the confidential data divided transmission scheme. According to the scheme the sender divides the original data into several parts which are independently transmitted via various communication channels, and the receiver reconstructs the original data from parts transmitted. To divide and reconstruct the data differential and integrated mathematical apparatus for polynomials in several variables over prime Galois fields is used, as well as Reed–Muller codes of the first and second orders. The correct work of the scheme provided that channels of proper quality are applied is proved. The scheme key space size and its redundancy estimations are computed. Application of the scheme provides both privacy and noise immunity of data transmitted which are its key distinctive features.*

Keywords*: divided transmission, Reed–Muller codes, confidential data, noise immunity, polynomials in several variables.*

References

3 Vladimir Deundyak (ORCID: 0000-0001-8258-2419), Ph.D., Associate Professor, Institute of mathematics, mechanics and computer Sciences southern Federal University, Rostov-on-don, Russia. E-mail: vl.deundyak@gmail.com

4 Nadia Mogilevskaya (ORCID: 0000-0003-1357-5869), Ph.D., Don state technical University, Rostov-on-don, Russia. E-mail: nadezhda.mogilevskaia@yandex.ru

1. Sklyar B. Tsifrovaya svyaz'. Teoreticheskie osnovy i prakticheskoe primenenie, 2-e izdanie. : Per. s angl. – Moscow, Izdatel'skiy dom «Vil'yams», 2016. 1104 p.
2. Cheremushkin A.V. Kriptograficheskie protokoly. Osnovnye svoystva i uyazvimosti. – Moscow, Izdatel'skiy tsentr «Akademiya», 2009. 272 p.
3. Mogilevskaya, N.S., Kul'bikayan, R.V., Zhuravlev L. A. Porogovoe razdelenie faylov na osnove bitovykh masok: ideya i vozmozhnoe primenenie. Vestnik Don. gos. tekh. un-ta. 2011, 11(10):1749-1755.
4. Tormasov, A.G., Khasin, M.A., Pakhomov, Yu.I. 2008. Obespechenie otkazoustoychivosti v raspredelennykh sredakh Rus. Programmirovanie. 27(5):26.
5. Mishchenko, V.A., Vilanskiy, Yu.V. Ushcherbnye teksty i mnogokanal'naya kriptografiya. Minsk: Entsiklopediks, 2007. 292 p.
6. Logachev O. A., Sal'nikov A. A., Yashchenko V. V. Bulevy funktsii v teorii kodirovaniya i kriptologii. – Moscow, MTsNMO, 2004. 470 p.
7. Deundyak, V. M., Knutova, A. V. Integriruemost' sistem polinomov neskol'kikh peremennykh pervoy i vtoroy stepeni nad prostymi polyami Galua, Izvestiya VUZov. Severo-Kavkazskiy region. Estestvennye nauki [University news. North-Caucasian region. Natural sciences series], 2016. 2(190):41–46.
8. Pellikaan, R., Wu, X.-W. List decoding of q-ary Reed-Muller Codes. Eng. IEEE Trans. On Information Theory, 2004. 50(3):679-682.
9. Deundyak, V. M., Mogilevskaya, N. S. Ob usloviyakh korrektnosti dekodera myagkikh resheniy troichnykh kodov Rida-Mallera vtorogo poryadka. Vladikavkazskiy matematicheskiy zhurnal [Vladikavkaz Mathematical Journal], 2016. 18(4): 23-33.
10. Sidel'nikov V.M. Teoriya kodirovaniya. – Moscow, FIZMATLIT, 2008. 324 p.
11. Gordeev E.N., Leont'ev V.K., Medvedev N.V. O svoystvakh bulevykh polinomov, aktual'nykh dlya kriptosistem, Voprosy kiberbezopasnosti [Cybersecurity issues], 2017. №3 (21). pp. 63-69.
12. Deundyak V.M., Maevskiy A.E., Mogilevskaya N.S. Metody pomekhoustoychivoy zashchity dannykh. Rostov-na-Donu, Izdatelstvo YuFU, 2014. 309 p.
13. Litsyn S.N., Shekhovtsov O.I. 1983. Bystryy algoritm dekodirovaniya kodov Rida-Mallera pervogo poryadka, Probl. peredachi inform. [Problems of Information Tansmission], 19(2):3–7.
14. Zyablov V.V., Portnoy S.L. 1991 Bystroe dekodirovanie kodov Rida–Mallera po maksimumu pravdopodobiya, Probl. peredachi inform. [Problems of Information Tansmission], 27(4):39–50.
15. Loidreau, P., Sakkour, B. Modified version of Sidel'nikov-Pershakov decoding algorithm for binary second order Reed-Muller codes. Ninth International Workshop on Algebraic and Combinatorial Coding theory, ACCT-9. Kranevo, 2004. Pp. 266-271.
16. Deundyak, V.M., Mogilevskaya, N.S. Model' troichnogo kanala peredachi dannykh s ispol'zovaniem dekodera myagkikh resheniy kodov Rida-Mallera vtorogo poryadka, Izvestiya vuzov. Severo-Kavkazskiy region. Tekhnicheskie nauki [University news. North-Caucasian region. Technical sciences series], 2015. № 1(182):3–10.