# СТОЙКОСТЬ ПОЛИНОМИАЛЬНОЙ СХЕМЫ РАЗДЕЛЕННОЙ ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

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

**Цель работы:** *исследование стойкости полиномиальной схемы разделенной передачи конфиденциальных данных к атакам на шифрограмму, ключ или часть ключа и расширение этой схемы на случай использования произвольных полей Галуа нечетной мощности. В схеме разделенной передачи конфиденциальных данных исходные данные на стороне отправителя разделяются на несколько частей и независимо друг от друга передаются по различным каналам связи, затем на стороне получателя из принятых частей восстанавливаются исходные данные.*

**Методы исследования:** *для расширения полиномиальной схемы на случай полей Галуа нечетной мощности использован математический аппарат линейной алгебры, теории полей Галуа и разделы общей теории полиномов нескольких переменных, связанные с их дифференцированием и интегрированием. Для исследования стойкости схемы разделенной передачи к атакам на шифрограмму и ключ сделано предположение, что нелегитимный пользователь системы передачи обнаружил уязвимость в технической защите одного или нескольких каналов легальных пользователей и организовал отводные каналы наблюдения.*

**Результаты:** *расширена на случай использования произвольных полей Галуа нечетной мощности полиномиальная схема разделенной передачи конфиденциальных данных, основанная на применении математического аппарата дифференцирования и интегрирования полиномов нескольких переменных над полями Галуа, а также кодов Рида-Маллера второго и первого порядков. Рассмотрены возможные атаки на схему в зависимости от числа организованных отводных каналов и количества перехваченных сообщений. Для случая однократного перехвата одного канала рассмотрена специальная атака, эффективная по отношению к атаке методом полного перебора, для нее получена грубая оценка сложности, а также оценено количество получаемых значений, «похожих» на искомые. Другие рассмотренные атаки строятся на основе атаки однократного перехвата одного канала. Проведенное исследование показало, что схема разделенной передачи конфиденциальных данных практически является стойкой.*

**Ключевые слова:** *атака на шифрограмму, атака на ключ, отводной канал, нелегитимный наблюдатель, декомпозиция данных, коды Рида-Маллера, полиномы нескольких переменных, параллельные каналы связи, защита данных.*

**DOI:** *10.21681/2311-3456-2018-4-38-45*

## 1. Введение и постановка задачи

В работе [1] построена теоретическая полиномиальная схема разделенной передачи (схема РП) конфиденциальных данных, в которой исходные данные на стороне отправителя разделяются на m частей и независимо друг от друга передаются по m различным каналам, а на стороне получателя из принятых частей восстанавливаются исходные данные. Для разделения и восстановления данных используется математический аппарат дифференцирования и интегрирования полиномов нескольких переменных над простыми полями Галуа, а также коды Рида-Маллера второго и первого порядков. Отличительная особенность схемы РП состоит в том, что ее использование обеспечивает как конфиденциальность, так и помехоустойчивость передаваемых данных.

В схеме РП есть два легитимных участника – отправитель и получатель. Цель легитимных участников – организация защищенной передачи конфиденциальных данных. Для определенности будем говорить, что отправитель и получатель используют систему связи, в которой есть m различных каналов. Согласно схеме [1] у отправителя и получателя есть секретный ключ $\beta = \{\bar{b}_i\}_{i=1,\dots,m}$ такой, что каждому из используемых каналов соответствует одна часть ключа $\bar{b}_i,\ i = 1,\dots,m$.

Назовем наблюдателем некоторого нелегитимного пользователя, который обнаружил уязвимость в технической защите одного или нескольких каналов легальных пользователей и организовал отводные каналы наблюдения. В общем случае отводной канал наблюдения можно рассматривать как перехват или как утечку информации вне зависимости от технических особен-

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

2 Могилевская Надежда Сергеевна, кандидат технических наук, доцент, доцент кафедры алгебры и дискретной математики Института математики, механики и компьютерных наук Южного федерального университета, г. Ростов-на-Дону, Россия. E-mail: nadezhda.mogilevskaia@yandex.ru; ORCID 0000-0003-1357-5869

ностей его организации, которые в данной работе не рассматриваются. Подобные системы с отводными каналами связи принято называть информационно-аналитическими системами канала наблюдения (см., например, [2-3]). Целью нелегитимного участника является как получение защищенных данных, так и получение части ключа $\beta$, соответствующей тому каналу системы связи, из которого организован отводной канал. Очевидно, что эффективность атаки наблюдателя зависит от количества организованных каналов наблюдения и от длительности их использования.

Цель настоящей работы состоит в расширении полиномиальной схемы разделенной передачи конфиденциальных данных из [1] на случай использования произвольных полей Галуа нечетной мощности, и исследовании стойкости схемы к атакам на шифрограмму, ключ или часть ключа.

## 2. Предварительные сведения и результаты

Введем необходимые обозначения. $F_q$ – конечное поле Галуа, $q=p^s$, $p$ – простое нечетное число, $s \in N$, $\mathbf{F}_q[x_1,...,x_m]$ – кольцо полиномов от переменных над полем $F_q$. Линейное пространство полиномов из $\mathbf{F}_q[x_1,...,x_m]$ степени не выше $r$ обозначим $\mathbf{F}_q^{(r)}[x_1,...,x_m]$. $\mathbf{F}_q^m$ – $m$-мерное линейное пространство над $F_q$.

В векторном пространстве $\mathbf{F}_q^m$ зафиксируем некоторое упорядочение

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

Произвольный информационный полином $f(\bar{x})\in \mathbf{F}_q^{(r)}[x_1,...,x_m]$ кодируется путем вычисления его значений в точках упорядоченного пространства $\mathbf{F}_q^m$:

$$C(f)=(f(\bar{\alpha}_1),...,f(\bar{\alpha}_n)), \quad (2)$$

и тем самым определяется оператор кодирования $C:\ \mathbf{F}_q^{(r)}[x_1,...,x_m]\to \mathbf{F}_q^n$.

Коды Рида-Маллера (РМ-коды) широко распространены [4-14] и могут быть заданы над произвольными полями Галуа. РМ-коды над конечным полем $F_q$ нечетной мощности (см. [13-14]) с информационными полиномами из $\mathbf{F}_q^{(r)}[x_1,...,x_m]$ и соответствующими информационными векторами $\bar{f}$ определяются натуральными параметрами $r$ и $m$, $m\ge r.0$, $m\ge 2$:

$$RM_q(r,m)=\{(f(\bar{\alpha}_1),...,f(\bar{\alpha}_n))\,|\,f(\bar{x})\in \mathbf{F}_q^{(r)}[x_1,...,x_m]\}\subset \mathbf{F}_q^n,$$

параметр $r$ называется порядком кода. РМ-коды образуют семейство линейных $[n,k,d]_q$-кодов, где $n=q^m$,

$$k=1+m,\ при\ \ r=1,\quad k=1+m+\frac{m(m+1)}{2},\ при\ \ r=2. \quad (3)$$

Способ вычисления параметра d кода можно найти, например, в [1, 13, 14].

По материалам [1, 15-16] кратко рассмотрим необходимые сведения о дифференцировании полиномов нескольких переменных. Производной полинома $f\in F_q^{(r)}[x_1,...,x_m]$ по направлению $\bar{b}\in \mathbf{F}_q^m$ называется результат действия оператора дифференцирования:

$$(D_{\bar{b}}f)(\bar{x})=f(\bar{x}+\bar{b})-f(\bar{x}),\ \ \bar{x}\in \mathbf{F}_q^m. \quad (4)$$

Легко показать, что $D_{\bar{h}}f\in \mathbf{F}_q^{(r-1)}[x_1,...,x_m]$, а оператор

$$D_{\bar{b}}:\ \mathbf{F}_q^{(r)}[x_1,...,x_m]\to \mathbf{F}_q^{(r-1)}[x_1,...,x_m] \quad (5)$$

является линейным.

В [13 с. 341-342] сформулирована и доказана следующая лемма.

**Лемма 1.** Пусть $q=p^s$, $f(\bar{x})\in \mathbf{F}_a^{(2)}[x_1,...,x_m]$, $\bar{b}=(b_1,...,b_m)\in \mathbf{F}_q^m$. Тогда $f(\bar{x})=f(\bar{0})+\bar{x}\left(f_{10...00},f_{01...00},...,f_{00...01}\right)^T+\bar{x}A\bar{x}^T$ (6)

$$(D_{\bar{b}}f)(\bar{x})=\bar{b}\left(f_{10...00},f_{01...00},...,f_{00...01}\right)^T+2\bar{x}A\bar{b}^T+\bar{b}A\bar{b}^T=2\bar{x}A\bar{b}^T+f(\bar{b})-f(\bar{0}), \quad (7)$$

где

$$A=\begin{pmatrix} f_{200..00} & f_{110..00}/2 & f_{101..00}/2 & K & f_{100..10}/2 & f_{100..01}/2 \\ f_{110..00}/2 & f_{020..00} & f_{011..00}/2 & K & f_{010..10}/2 & f_{010..01}/2 \\ f_{101..00}/2 & f_{011..00}/2 & f_{002..00} & K & f_{001..10}/2 & f_{001..01}/2 \\ K & K & K & 0 & K & K \\ f_{100..10}/2 & f_{010..10}/2 & f_{001..10}/2 & K & f_{000..20} & f_{000..11}/2 \\ f_{100..01}/2 & f_{010..01}/2 & f_{001..01}/2 & K & f_{000..11}/2 & f_{000..02} \end{pmatrix}.$$

Рассмотрим аналог оператора дифференцирования $D_{\bar{b}}$ [1, 13, 15], действующего в пространстве полиномов (см.(1)), для пространства $\mathbf{F}_q^n$, где $n=q^m$. Определим оператор сдвига $\tau_{\bar{h}}:\mathbf{F}_q^n\to\mathbf{F}_q^n$, формулой

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

где $\bar{a}=(a_{\bar{\alpha}_1},...,a_{\bar{\alpha}_n})\in \mathbf{F}_q^n$, $\bar{b}=(b_1,...,b_m)\in \mathbf{F}_q^m$, $\Delta_{\bar{b}}:\mathbf{F}_q^n\to\mathbf{F}_q^n$. Линейный оператор ,определим формулой:

$$\Delta_{\bar{b}}(\bar{a})=\tau_{\bar{b}}(\bar{a})-\bar{a},\ \bar{a}=(a_{\bar{\alpha}_1},...,a_{\bar{\alpha}_n})\in \mathbf{F}_q^n, \quad (8)$$

назовем производным вектором вектора $\Delta_{\bar{b}}(\bar{a})$ по направлению $\bar{b}$ [1, 15]. Легко видеть, что для полинома $f\in \mathbf{F}_q^{(2)}[x_1,x_2,...,x_m]$, вектора $\bar{b}\in \mathbf{F}_q^m$, операторов $\Delta_{\bar{b}}$, $D_{\bar{b}}$ и справедливо

$$\tau_b(C(f))=C(f_b),\ C(D_bf)=\Delta_b(C(f)).. \quad (9)$$

Формула (9) доказывается прямыми выкладками, аналогичные утверждения для случая простых полей сформулированы и доказаны в [1, 13].

## 3. Схема разделенной передачи конфиденциальных данных

В работе [1] рассмотрена полиномиальная схема РП, организованная на основе применения простых полей Галуа. В этом разделе схема из [1] модифицирована на случай произвольных полей Галуа нечетной мощности. Доказательство корректности схемы легко провести по схеме доказательства из [1] с использованием математических результатов из [14].

В полиномиальной схеме для разделения и восстановления данных используются $[n, k_1, d_1]_q$-код $RM_q(1,m)$ и $[n, k_2, d_2]_q$-код $RM_q(2,m)$, заданные над полем Галуа $F_q$ нечетной мощности, где $q=p^r$, $p$ - простое, $r$ - натуральное. Значения и являются параметрами схемы. Основными этапами работы схемы (рис. 1) являются разделение исходного сообщения на частей, передача этих частей по различным каналам и восстановление сообщения.

Построим алгоритм разделения сообщений

АЛГОРИТМ 1.

Вход: информационный вектор $\bar{f}\in \mathbf{F}_q^{k_2}$, упорядоченный набор базисных векторов

$$\beta=\{\bar{b}_i=(b_1^i,b_2^i,...,b_m^i)\in \mathbf{F}_q^m\}_{i=1,...,m}, \quad (10)$$

который является секретным ключом рассматриваемой схемы.

Выход: набор векторов $\bar{S}_i\in \mathbf{F}_q^{n+1}$, $i=\overline{1,m}$.

Шаг 1. С использованием (2) вычисляется кодовый вектор $\bar{S}_i\in \mathbf{F}_q^{n+1}$, $i=\overline{1,m}$ кода $RM_q(2.m)$, $f=f(\bar{x})$ – информационный полином, соответствующий $\bar{f}$.

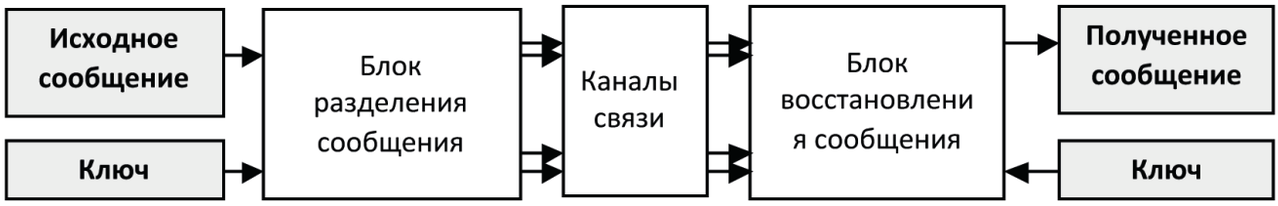



*Рис. 1. Основные элементы схемы распределенной передачи данных*

Шаг 2. Вычисляются векторов вида (см. (8)):

$$\Delta_{\bar{b}_i}(C(f)) = C(D_{\bar{b}_i}(f)) \in \mathbf{F}_q^n,\ i=\overline{1,m},\ \bar{b}_i \in \beta.$$

Отметим, что $C(D_{\bar{b}_i}(f)) \in RM_a(1,m)$.

Шаг 3. Каждый вектор $C(D_{\bar{b}_i}(f)) \in \mathbf{F}_q^n$, $i=\overline{1,m}$ конкатенируется с коэффициентом $f_{00..00} := f(\bar{0})$ кодового вектора $C(w)$:

$$\bar{S}_i = C(D_{\bar{b}_i}(f)) \,\|\, f_{00..00} \in \mathbf{F}_q^{n+1}.$$

Затем векторы $\bar{S}_i$, $i=\overline{1,m}$, передаются по различным каналам связи. Очевидно, что во время передачи векторы $\bar{S}_i$, $i=\overline{1,m}$, могут быть искажены. Таким образом, на стороне получателя будут получены векторы $\bar{S}_i'$:

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

где $(C(D_{\bar{b}_i}(f)))'$ и $f'_{00..00}$ – возможно искаженные вектор $C(D_{\bar{b}_i}(f))$ и скаляр $f'_{00..00}$. Скаляр $f'_{00..00}$ соответствующий $\bar{S}_i'$ обозначим $f'_{00..00,i}$.

Построим алгоритм восстановления сообщения.

АЛГОРИТМ 2.

Вход: векторы $\bar{S}_i$, $i=\overline{1,m}$, секретный ключ $\beta$ (см. (10)).

Выход: вектор $\bar{f} \in \mathbf{F}_q^{k_2}$.

Шаг 1. Из каждого вектора $\bar{S}_i$, $i=\overline{1,m}$, выделяется вектор $(C(D_{\bar{b}_i}(f)))' \in \mathbf{F}_q^n$ и скаляр $f'_{00..00,i}$, $i=\overline{1,m}$.

Шаг 2. Векторы $(C(D_{\bar{b}_i}(f)))'$ декодируются произвольными декодерами кода $RM_q(1,m)$. На выходе декодеров формируются полиномы $D'_{\bar{b}_i}(f) \subset \mathbf{F}_q^{(1)}[x_1,x_2,...,x_m]$, $i=1,...,m$.

Шаг 3. Из коэффициентов $f_{00..00,i}$, полученных на шаге 1,создается вектор $(f'_{00..00,1}, f'_{00..00,2}, ..., f'_{00..00,m})$ и обрабатывается мажоритарным декодером кода $RM_q(0,m)$ Результатом декодирования является скаляр $f''_{00..00}$.

Шаг 4. Из элементов ключа $\beta = \{b_i = (b_i^1, b_i^2, ..., b_i^m)\}$ и коэффициентов полиномов $\left\{\left(D_{\bar{b}_i} f\right)(\bar{x}) = \alpha_1^i x_1 + \alpha_2^i x_2 + ... + \alpha_m^i x_m + \alpha_0^i\right\}_{i=\overline{1,...,m}} \subset \mathbf{F}_p^{(1)}[x_1,x_2,...,x_m]$, строится искомый информационный полином $f(\bar{x}) = f''_{00..00} + \bar{x}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + \bar{x}A\bar{x}^T$,

где матрица вычисляется по формуле

$$A = \tfrac{1}{2}\Omega B^{-1},$$

$$B = (b_j^i)_{i,j=\overline{1,m}} = \begin{pmatrix} b_1^1 & b_1^2 & \cdots & b_1^m \\ b_2^1 & b_2^2 & \cdots & b_2^m \\ \vdots & \vdots & \ddots & \vdots \\ b_m^1 & b_m^2 & \cdots & b_m^m \end{pmatrix},\quad \Omega = (\alpha_j^i)_{i,j=\overline{1,m}} = \begin{pmatrix} \alpha_1^1 & \alpha_1^2 & \cdots & \alpha_1^m \\ \alpha_2^1 & \alpha_2^2 & \cdots & \alpha_2^m \\ \vdots & \cdots & \ddots & \vdots \\ \alpha_m^1 & \alpha_m^2 & \cdots & \alpha_m^m \end{pmatrix},$$

а вектор $(f_{10...00}, f_{01...00}, ..., f_{00...01})$ находится из равенства

$$(f_{10...00}, f_{01...00}, ..., f_{00...01})^T = \left(\alpha_0^1 - b_1 A b_1^T, \alpha_0^2 - b_2 A b_2^T, ..., \alpha_0^m - b_m A b_m^T\right)B^{-1}.$$

Шаг 5. Получателю сообщений выдается информационный вектор $\bar{f} \in \mathbf{F}_q^{k_2}$, соответствующий полиному $f(\bar{x})$.

В работе [1] (см. также [14, с. 341-342]), сформулирована и доказана теорема об условиях, корректности схемы РП, а именно вектор $\bar{f}$, полученный на выходе блока восстановления сообщения, совпадет с исходным информационным вектором $\bar{w}$, если выполняются следующие условия:

1) $\forall i=\overline{1,m}$: $d_H(C(D_{\bar{b}_i}(w)), (C(D_{\bar{b}_i}(w)))') \le \lfloor (d_1-1)/2 \rfloor$, (11)

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

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 $f_{00..00} = w(\bar{0})$.

В случае, когда в используемых каналах связи произошло ошибок больше, чем могут исправить декодеры, восстановление информационного вектора не гарантируется.

**4. Стойкость полиномиальной схемы РП**

Предположим, что наблюдатель обнаружил уязвимость в одном или нескольких каналах связи легальных пользователей и организовал отводные каналы наблюдения, для которых выполняются условия корректности полиномиальной схемы РП, в частности условие (11). Далее будем считать, что наблюдатель, как и легальный пользователь, умеет определять начало и конец векторов $\bar{S}_i'$, полученных из отводных каналов, и знает упорядочение (1). Оценим стойкость схемы РП к возможным атакам наблюдателя в зависимости от количества отводных каналов и числа перехваченных векторов $\bar{S}_i'$, отметим, что для случая простых полей некоторые из таких атак упомянуты в [1].

4.1.Рассмотрим однократный перехват из $i$-того канала связи, т.е. ситуацию, когда нелегальному наблюдателю удается получить вектор $\bar{S}_i' = (C(D_{\bar{b}_i}(f)))' \,\|\, f'(\bar{0}) \in \mathbf{F}_q^{n+1}$ .Для упрощения обозначений положим: $\bar{b} = \bar{b}_i$, этот вектор является частью ключа $\beta$.

Предположим, что часть ключа, соответствующая перехваченному каналу связи, т.е. вектор $\bar{b} = \bar{b}_i$, неизвестен. В этом случае наблюдатель может рассмотреть атаки на информационный вектор $\bar{f}$ и часть ключа $\bar{b}$. Ниже покажем, что в такой ситуации эти атаки неотделимы друг от друга и выполняются одновременно. С точки зрения криптографии это атаки на шифротекст и на ключ [17, с. 20-21].

Атакующий по вектору $\bar{S}_i'$ с помощью декодера кода может вычислить $D_{\bar{b}}(f)$, а затем ему необходимо решить задачу нахождения информационного

полинома $f \in \mathbf{F}_q^{(2)}[x_1, x_2, ..., x_m]$ и вектора $\bar{b} \in \mathbf{F}_q^m$. Очевидно, что кроме искомых $f$ и $\bar{b}$ могут найтись другие значения $\varphi \in \mathbf{F}_q^{(2)}[x_1, x_2, ..., x_m]$ и $\bar{v}(\in \mathbf{F}_q^m)$, для которых $D_{\bar{b}}(f) = D_{\bar{v}}(\varphi)$. Такие значения $(\varphi, \bar{v})$ будем называть *подходящей парой*. Опишем ниже два способа построения списка подходящих пар и оценим их сложность. Отметим, что в случае однократного перехвата у наблюдателя нет возможности выбрать из списка подходящих пар единственно верную, если, конечно, наблюдатель не обладает некоторыми дополнительными сведениями об исходном сообщении.

Первый способ поиска подходящих пар состоит в полном переборе всех возможных векторов $\bar{v} \in \mathbf{F}_q^m$ и полиномов $\varphi \in \mathbf{F}_q^{(2)}[x_1, x_2, ..., x_m]$ и нахождении в них тех, для которых справедливо $D_{\bar{b}}(f) = D_{\bar{v}}(\varphi)$. Вектор $\bar{v}$ содержит $m$ координат, полином $\varphi$ содержит $k = 1 + m + \frac{m(m+1)}{2}$ коэффициентов, таким образом, при полном переборе для поиска подходящих пар $(\varphi, \bar{v})$ необходимо рассмотреть

$$q^k q^m = q^{2m + \frac{m(m+1)}{2} + 1} \quad (12)$$

вариантов $\varphi$ и $\bar{v}$.

Рассмотрим второй способ поиска подходящих пар. Пусть $a(\bar{x}) = a_0 + <\bar{x}, \bar{u}> -$ – результат правильного декодирования наблюдателем вектора $(C(D_{b_i}(f)))'$, т.е. $D_{\bar{b}}(f) = a(\bar{x})$. Пусть $\bar{a} = (a_0, \bar{u})$. В силу (7) из равенства $D_{\bar{b}}(f) = a(\bar{x})$ получаем

$$2\bar{x}A\bar{b}^T + f(\bar{b}) - f(\bar{0}) = a_0 + <\bar{x}, \bar{u}>,$$

следовательно, для нахождения подходящих пар можно рассмотреть нелинейную систему из $m+1$ уравнений с $2m + \frac{m(m+1)}{2} + 1$ неизвестными, среди которых $m$ координат вектора $\bar{b}$ и $1+m+m(m+1)/2$ коэффициентов $f$:

$$\begin{cases} f(\bar{b}) - f(\bar{0}) = a_0, \\ 2A\bar{b}^T = \bar{u}^T. \end{cases} \quad (13)$$

Отметим, что система (13) нелинейная и недоопределенная, а ее разрешимость следует из того, что пара $(f, \bar{b})$ является одним из ее решений. Используем (6) и перепишем систему (13):

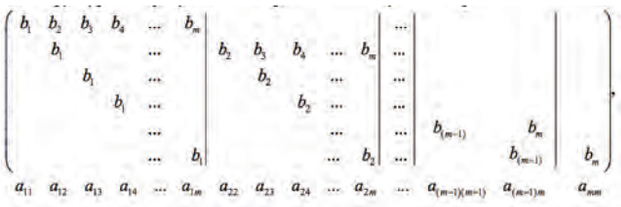
$$\begin{cases} \bar{b}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + \bar{b}A\bar{b}^T = a_0, \\ 2A\bar{b}^T = \bar{u}^T, \\ \bar{b}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T = a_0 - \frac{1}{2}\bar{b}\bar{u}^T, \\ A\bar{b}^T = \frac{1}{2}\bar{u}^T. \end{cases} \quad (14)$$

Рассмотрим матричное уравнение $A\bar{b}^T = \frac{1}{2}\bar{u}^T$ в случае, когда матрица A неизвестна, а кроме вектора $\bar{u}$ известен и вектор $\bar{b}$. Тогда относительно элементов матрицы A получаем линейную систему $M$, содержащую $m$ уравнений с $\frac{m(m+1)}{2}$ неизвестными элементами матрицы $A$, которую можно решить, например, методом Гаусса. Покажем, что система $M$ имеет решение для произвольного значения вектора $\bar{b}$. Упорядочим неизвестные элементы матрицы $A$ естественным лексикографическим способом, учитывая симметричность матрицы:

$a_{11}, a_{12}, ..., a_{1m}, a_{22}, a_{23}, ..., a_{2m}, ..., a_{kk}, a_{k(k+1)}, ..., a_{km}, ..., a_{mm}$.

Через $B$ обозначим матрицу системы $M$.

Матрица $B$ имеет следующую структуру: первые $m$ столбцов образуют верхнетреугольную матрицу, на диагонали которой стоят элементы $b_1$, первая строка представляет собой последовательность $b_1, b_2, ..., b_m$, а остальные элементы равную нулю. Следующие столбцов образуют матрицу, у которой верхняя строка равна нулю, вторая строка содержит элементы $b_2, b_3, ..., b_m$, а на местах, соответствующих элементам $a_{23}, a_{23}, ... a_{2m}$, находятся элементы $b_2$ и т.д. Структурно матрицу $B$ можно представить следующим образом:



где незаполненные позиции соответствуют нулям в матрице $B$, а в нижней дополнительной строке указаны искомые элементы матрицы $A$, соответствующие столбцам матрицы $B$. Например, для $m=3$ система $M$ выглядит следующим образом:

$$\begin{cases} a_{11}b_1 + a_{12}b_2 + a_{13}b_3 = \frac{1}{2}u_1, \\ a_{12}b_1 + a_{22}b_2 + a_{23}b_3 = \frac{1}{2}u_2, \\ a_{13}b_1 + a_{23}b_2 + a_{33}b_3 = \frac{1}{2}u_3. \end{cases}$$

Вычислим ранг матрицы $B$.

Лемма. rank(B) = $m$.

Доказательство. Рассмотрим подматрицу $D$ матрицы $B$, составленную из первых $m$ столбцов. Выше было показано, что она удовлетворяет следующим условиям:

1) первая строка это координаты вектора $\bar{b}$,

2) на диагонали матрицы стоит первая координаты вектора $\bar{b}$,

3) остальные элементы равны нулю.

Предположим, что $\bar{b} \neq 0$. В этом случае искомое равенство вытекает из структуры матрицы $D$.

Предположим, что $b_1 = 0$, тогда найдется $b_k \neq 0$ для некоторого $k$. Этот случай легко сводится к случаю $b_1 \neq 0$. Действительно, надо в матрице $B$ поменять местами первую и $k$-тую строки и переставить столбцы таким образом, что бы первые $m$ столбцов образовали верхнетреугольную матрицу, на диагонали которой стоят элементы $b_k$, первая строка представляла собой последовательность $b_1, b_2, ..., b_m$, с переставленными элементами $b_1$ и $b_k$, а остальные элементы равную нулю. •

Из леммы вытекает, что система $M$ имеет решение для произвольного значения вектора $\bar{b}$. Рассмотрим алгоритм решения системы (14), основанный на переборе всевозможных значений векторов $\bar{b}$.

АЛГОРИТМ 3.

Вход: $\bar{a}=(a_0, \bar{u})$, $m$, $q$.

Выход: список $L$ длиной $q^m \frac{m(m+1)}{2}$ подходящих пар $(\varphi, \bar{b}_1)_1, (\varphi, \bar{b}_1)_2, ..., (\varphi, \bar{b}_1)_r$, $(\varphi, \bar{b}_2)_1, (\varphi, \bar{b}_2)_2, ..., (\varphi, \bar{b}_2)_r, ..., (\varphi, \bar{b}_{q^m})_1 (\varphi, \bar{b}_{q^m})_2, ..., (\varphi, \bar{b}_{q^m})_r$, где

$r = \frac{m(m+1)}{2}$, $\bar{b}_s \in \mathbf{F}_q^m$, $s = \overline{1, q^m}$ а $\varphi$, а $\varphi$ – это некоторые полиномы из $\mathbf{F}_q^{(2)}[x_1, x_2, ..., x_m]$.

Шаг 1. Рассмотрим всевозможные векторы $\bar{b} \in \mathbf{F}_q^m$, и выполним для каждого из них шаги 2-4 алгоритма.

Шаг 2. Для фиксированного значения вектора $\bar{b}$ решаем первое уравнение системы (14), являющееся линейным с $m$ неизвестными $f_{10...00}, f_{01...00}, \ldots, f_{00...01}$. Получаем множество $\Lambda_{\bar{b}}^1 = \{(f_{10...00}, f_{01...00}, \ldots, f_{00...01})_k\}_{k=1}^{L_{\bar{b}}}$, где $L_{\bar{b}} = q^{m-1}$,его решений как линейное многообразие размерности *(m-1)*. элементы которого зависят от $\bar{b}$ :

$$\begin{cases} f_{1000}, \ldots, f_{0010} \in F_q \\ f_{0001} = a_0 - \frac{1}{2}\sum_{i=1}^{m} b_i u_i - (b_1 f_{1000} + \ldots + b_{m-1} f_{0010}) \end{cases}.$$

Шаг 3. Для фиксированного значения вектора $\bar{b}$ методом Гаусса решаем уравнение $Ab^T = \frac{1}{2}u^T$ относительно элементов матрицы *A* и находим множество всех его решений $\Lambda_{\bar{b}}^2 = \{\Psi_k\}_{k=1}^{M_{\bar{b}}}$, где $M_{\bar{b}} = \frac{m(m+1)}{2} - m$.

Шаг 4. Для фиксированного значения вектора $\bar{b}$ формируем $q^{\frac{m(m+1)}{2}-m} q^{m-1} q = q^{\frac{m(m+1)}{2}}$ всевозможные подходящие пары вида ( $\varphi, \bar{b}$ ) где $\varphi$ – это полином вида

$$\varphi(\bar{x}) = \varphi(\bar{0}) + \bar{x}\left(f_{10...00}, f_{01...00}, \ldots, f_{00...01}\right)^T + \bar{x}A\bar{x}^T$$

(см. (6)), в состав полинома входят скаляр $\varphi(\bar{0}) (\in F_a)$,вектор $\left(f_{10...00}, f_{01...00}, \ldots, f_{00...01}\right) \in \Lambda_{\bar{b}}^1$, матрица $A \in \Lambda_{\bar{b}}^2$. •

Существование решения вытекает из леммы о ранге матрицы *B*.

Замечание. Из алгоритма 3 видно, что для фиксированного значения $\bar{b}$ существует $q^{m-1}$ значений вектора $(f_{1000}, \ldots, f_{0010})$, которые удовлетворяют первому уравнению системы (14), и для произвольного частичного ключа $\bar{b}$ мы можем найти $q^{\frac{m(m+1)}{2}-m}$ вариантов матрицы *A*.

**Теорема.** В результате однократного перехвата одного канала, наблюдатель со сложностью $O(q^m(m+1)^3)$ может получить список из $q^{m+\frac{m(m+1)}{2}+1}$ подходящих пар.

Доказательство. Выше показано, что для нахождения подходящей пары по результату однократного перехвата одного канала, наблюдатель может использовать построенный алгоритм решения системы (14).Нестрого оценим сложность этого алгоритма. На шаге 3 алгоритма решается система уравнений методом Гаусса, сложность которого оценивается как $O(n^3)$, где $n$ – количество уравнений в системе. Система (14) содержит $m+1$ уравнений, в ходе выполнения алгоритма ее необходимо решить для каждого $\bar{b} \in \mathbf{F}_q^m$, т.е. $q^m$ раз. Следовательно, сложность алгоритма 3 можно примерно оценить, как $O(q^m(m+1)^3)$.

Определим длину списка подходящих пар. Каждая пара содержит вектор из пространства $\mathbf{F}_q^m$ (таких векторов ) и полином из пространства $\mathbf{F}_a^{(2)}[x_1, x_2, \ldots, x_m]$ вида (6)

$$f(\bar{x}) = f(\bar{0}) + \bar{x}\left(f_{10...00}, f_{01...00}, \ldots, f_{00...01}\right)^T + \bar{x}A\bar{x}^T.$$

При выполнении алгоритма 3 решения системы (14) этот полином восстанавливается по частям. Из замечания к алгоритму вытекает, что на шаге 2 алгоритма находится $q^{m-1}$ значений вектора $(f_{1000}, \ldots, f_{0010})$, а на шаге 3 находится $q^{\frac{m(m+1)}{2}-m}$ вариантов матрицы *A*. Алгоритм восстанавливает полином $f(\bar{x})$ без свободного члена, следовательно, необходимо рассмотреть еще $q$ значений для $f(\bar{0})$. Итого получаем $q^{\frac{m(m+1)}{2}+m} = q^m q^{\frac{m(m+1)}{2}-m} q^{m-1} q$ подходящих пар. •

Отметим, что использование второго способа поиска подходящих пар уменьшает перебор при поиске с $q^{2m+\frac{m(m+1)}{2}+1}$ возможных пар (см. (12)) до $q^{\frac{m(m+1)}{2}+m}$. При этом уменьшение перебора в $q^m$ раз происходит за счет второго уравнения системы (14), а уменьшение в $q$ раз происходит за счет решения первого уравнения системы.

4.2. Рассмотрим однократный перехват из *i*-го канала в случае, когда наблюдателю известна часть ключа $\bar{b}$, соответствующая этому каналу. Тогда при использовании наблюдателем метода полного перебора для нахождения подходящих пар ему необходимо рассмотреть

$$p^k = p^{m+\frac{m(m+1)}{2}+1}$$

вариантов значений $\varphi \in \mathbf{F}_q^{(2)}[x_1, x_2, \ldots, x_m]$ отыскивая среди них те, для которых верно равенство $D_{\bar{b}}(f) = D_{\bar{v}}(\varphi)$, где значение $D_{\bar{b}}(f)$, вычислено по вектору $\bar{S}_{i_1}'$ с помощью декодирования. Использование алгоритма 3 потребует от наблюдателя только одного прохода, т.к. вектор $\bar{b}$ известен. Используя алгоритм 3, наблюдатель из первого уравнения системы находит $q^{m-1}$ значений вектора $(f_{1000}, \ldots, f_{0010})$, а затем подставляет вектор $\bar{b}$ во второе уравнение системы с $\frac{m(m+1)}{2}$ неизвестными, которую необходимо решить. Из доказательства теоремы легко видеть, что результатом работы алгоритма будет список из $p^{\frac{m(m+1)}{2}}$ подходящих пар.

4.3. Рассмотрим ситуацию *t*-кратного перехвата одного канала. Наблюдатель, применяя к каждому из полученных значений $\bar{S}_{i_1}', \ldots, \bar{S}_{i_t}'$. рассмотренную выше атаку на основе однократного перехвата (см. алгоритм 3), получит $t$ различных списков подходящих пар, длиной $q^{m+\frac{m(m+1)}{2}+1}$ каждый. В каждом из списков найдутся всевозможные значения вектора $\bar{b}$ – кандидата на роль частичного ключа и каждому из них будет соответствовать список из $\frac{m(m+1)}{2}$ полиномов $\varphi$. Полученные результаты не позволяют уменьшить перебор по сравнению со случаем 5.1, т.к. не имея каких-либо дополнительных сведений о передаваемых данных, выбрать верные полиномы из полученных списков невозможно.

4.4. Рассмотрим однократный перехват из $\mu$ $(2 < \mu < m)$ различных каналов. В этом случае наблюдатель получит векторы $\bar{S}_{ij}'$, $j = 1, \ldots, \mu$, , соответствующие одному и тому же информационному полиному $f$. Используя алгоритм поиска подходящих пар, он сможет построить $\mu$ списков: $L_1$, $L_2$, ...., $L\mu$, при этом в силу теоремы длина каждого списка $q^{m+\frac{m(m+1)}{2}+1}$ пар. Из полученных списков подходящих пар наблюдатель может составить наборы вида

$$\Omega = (\sigma \in \mathbf{F}_q^{(2)}[x_1, x_2, \ldots, x_m], \Gamma = \{\bar{\gamma}_i \in \mathbf{F}_q^m\}_{i=1,\ldots,\mu}),$$

где $\sigma$ - кандидат на роль искомого информационного полинома $f \in \mathbf{F}_q^{(2)}[x_1, x_2, \ldots, x_m]$, а $\Gamma$ – кандидат на роль частично восстановленного ключа $\beta$ (см. (10)), при этом в $\Gamma$ – присутствует $\mu < m$ элементов.

Рассмотрим схему алгоритма создания наборов $\Omega$ по спискам $L_1$, $L_2$, ...., $L\mu$ подходящих пар. Зафиксируем полином $\varphi_1$ из первой пары списка $L_1$ и отыщем все пары $(\varphi_1, \bar{b}_{s_2})^{L_2}, \ldots, (\varphi_1, \bar{b}_{s_\mu})^{L_\mu}$ в других списках, содержащих полином $\varphi_1$. Если не удалось найти такие пары во всех списках, то удаляем все найденные пары с полиномом $\varphi_1$ из всех списков. Если такие пары нашлись во всех списках

$$(\varphi_1, \bar{b}_{s_1})^{L_1}, \ldots, (\varphi_1, \bar{b}_{s_\mu})^{L_\mu},$$

и совокупность векторов из этих пар линейно независима, то формируем новый набор $\Omega$, содержащий полином $\varphi_1$ и множество $\Gamma = \{\bar{b}_{s_j}\}_{j=\overline{1,\mu}}$. Теперь удаляем найденные пары $(\varphi_1, \bar{b}_{s_1})^{L_1}, ..., (\varphi_1, \bar{b}_{s_\mu})^{L_\mu}$ из всех списков и повторяем проведенные действия для каждого из оставшихся полиномов до тех пор, пока списки пар не пустые. Таким образом, в рассматриваемой ситуации при удачном сочетании данных и ключа с ростом $\mu$ возможно значительное уменьшение длины списка подходящих пар, вплоть до восстановления $\mu$ частичных ключей системы. Последнее обстоятельство позволяет после этого проводить атаки из пункта 5.2 для каждого из рассматриваемых $\mu$ каналов.

4.5. Рассмотрим атаку на ключ на основе подобранного открытого текста [17, с.20-21]. Предположим, что наблюдатель может навязать отправителю некоторое информационное сообщение $\bar{f}$ и контролирует один или несколько каналов передачи данных. Для однозначного восстановления части ключа $\bar{b}$, связанного с конкретным каналом, достаточно, чтобы матрица *A*, составленная из коэффициентов $\bar{f}$ (см. (6)), была обратима (см. второе уравнение системы (14)). Найденный ключ $\bar{b}$ позволяет далее проводить атаки из пункта 5.2 и упрощает атаки из пункта 5.4. Если же наблюдатель не может навязать удобное для атаки информационное сообщение $\bar{f}$, но ему удается передаваемое сообщение узнать, то вектор $\bar{b}$ может восстанавливаться неоднозначно: если *rank(A)=r*, то множество решений является линейным многообразием размерности *m-r*.

**Выводы**

В работе полиномиальная схема разделенной передачи данных из [1] расширена на случай использования произвольных полей Галуа нечетной мощности и проведено исследовании стойкости схемы к атакам на шифрограмму, ключ или часть ключа.

В случаях однократного перехвата из одного канала связи, как при известном, так и при неизвестном частичном ключе (см. разделы 5.1 и 5.2), получены оценки на длины получаемых в результате атаки списков подходящих пар, которые позволяют сделать вывод о том, что система РП достаточно защищена. Показано, что несколько перехватов в одном канале (раздел 5.3), без каких-либо дополнительных сведений о передаваемых данных, успешность атаки не увеличивает.

Наиболее успешной оказалась атака, организованная с помощью однократного перехвата из $\mu$ ($2<\mu<m$) различных каналов (раздел 5.4),при удачном сочетании данных и ключа с ростом числа отводных каналов возможно значительное уменьшение длины списка подходящих пар, вплоть до восстановления частичных ключей системы. В разделе 5.5 описан способ нахождения частичного ключа, в случае, когда наблюдателю удается навязать сообщение легальному отправителю. Известное значение частичного ключа позволяет проводить атаки из раздела 5.2 и упрощает атаки из раздела 5.4.

***Рецензент:*** Марков Алексей Сергеевич, доктор технических наук, старший научный сотрудник, профессор Московского государственного технического университета им. Н.Э.Баумана, Москва, Россия.
E-mail: a.markov@npo-echelon.ru.

***Литература***

1. Деундяк В.М., Могилевская Н.С. Схема разделенной передачи конфиденциальных данных на основе дифференцирования полиномов нескольких переменных над простыми полями Галуа // Вопросы кибербезопасности. 2017. №5 (24). С.64-71. DOI: 10.21681/2311-3456-2017-5-64-71.
2. Косолапов Ю.В. Метод кодового зашумления в задачах защиты информации.-Ростов-на-Дону: ЮФУ, 2014. 164 с.
3. Букашкин С.А. Метод случайного кодирования // Радиотехника. 2014. №4. С. 31-36.
4. Fukumoto S., Wadayama T. Iterative erasure correcting algorithm for q-ary Reed-Muller codes based on local correctability. 9th International Symposium on Turbo Codes and Iterative Information Processing (ISTC IEEE). (Brest, France, 5-9 Sept., 2016). Pp. 36 – 40. DOI: 10.1109/ISTC.2016.7593072.
5. Kudekar S., Kumar S., Mondelli M., Pfister H. D., Sasoglu E., Urbanke R. Reed-Muller codes achieve capacity on erasure channels. IEEE Trans. Inform. Theory, vol. 63, no. 7, pp. 4298-4316, 2017.
6. Santi E., Hager C. Pfister H. Decoding Reed-Muller Codes Using Minimum-Weight Parity Checks. IEEE International Symposium on Information Theory (ISIT). 2018. Pp. 1296 – 1300.
7. Saptharishi R., Shpilka A., Volk B. L. Efficiently decoding Reed–Muller codes from random errors. Proc. 48th Annu. ACM Symp. Theory Comput. (STOC), pp. 227-235, 2016, http://doi.acm.org/10. 1145/2897518.2897526.
8. Young Gil Kim, A. J. Han Vinck. 4-Ary Codebook Design Using Reed–Muller Codes for MIMO Beamforming Systems. IEEE Transactions on Vehicular Technology (Vol. 65, Issue: 2, Feb. 2016). Pp. 959 – 966. DOI: 10.1109/TVT.2015.2404844.
9. Козловский А.В., Насыров А.М. Специфика применения структурных особенностей кодовых комбинаций полярных кодов и кодов Рида-Маллера Современные проблемы проектирования, производства и эксплуатации радиотехнических систем. 2017. № 1-2 (10). С. 159-161.
10. Бородин М.А., Чижов И.В. Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида-Маллера Дискретная математика. 2014. Т. 26. № 1. С. 10-20.
11. Деундяк В.М., Могилевская Н.С. Восстановление данных из отводного канала наблюдения с использованием декодеров, работающих за пределом половины кодового расстояния // Телекоммуникации. 2017. № 4. С. 27-33.
12. Деундяк В.М., Могилевская Н.С. Об использовании мягких и вероятностных декодеров для восстановления данных при перехвате // Известия высших учебных заведений. Северо-Кавказский регион. Серия: Естественные науки. 2017. № 1

(193). С. 18-24.
13. 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.
14. Деундяк В.М., Могилевская Н.С. Дифференцирование полиномов нескольких переменных над полями Галуа нечетной мощности и приложения к кодам Рида-Маллера. Вестник Донского государственного технического университета. 2018. № 18(3) С. 339-348. DOI: 10.23947/1992-5980-2018-18-3-339-348.
15. 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.
16. 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.
17. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М.: Триумф, 2016. – 816 с.

# RESISTANCE OF THE POLYNOMIAL SCHEME OF CONFIDENTIAL DATA SPLIT TRANSMISSION

***Deundyak V.M.[1], Mogilevskaya N.S.[2]***

***Purpose:*** *Study the resistance of a polynomial scheme of confidential data split transmission to attacks on a cipher, key or part thereof, and the extension of this scheme when using arbitrary Galois fields of odd power. In the confidential data split transmission scheme, the sender edge source data is divided into several parts and transferred independently via different communication channels. Then on the recipient edge, the original data is restored from the parts received.*

***Research methods:*** *In order to extend the polynomial scheme to the case of Galois fields of odd power, use was made of the linear algebra mathematical apparatus, Galois field theories and sections of the general theory of polynomials of several variables, related to their differentiation and integration. To investigate the resistance of the divided transfer scheme to attacks on a cipher and key, it was assumed that an illegitimate user of the transmission system discovered vulnerability in the technical protection of one or several channels of legitimate users and organized wiretap surveillance channels.*

***Results:*** *Extended to using arbitrary Galois fields of odd power was the polynomial scheme for confidential data split transmission based on the use of mathematical apparatus for differentiating and integrating polynomials of several variables over Galois fields, as well as second- and first-order Reed-Muller codes. Possible attacks on the scheme depending on the number of organized wiretap channels and intercepted messages are considered. For a single intercept of one channel, a special attack effective in relation to a brute-force attack was considered and roughly estimated for complexity; also estimated was the number of obtained values "similar" to the sought ones. The other attacks under review build on a single intercept attack on one channel. The study showed that the confidential data split transmission scheme is actually resistant.*

***Keywords:*** *an attack on the cipher, attack on the key, branch channel, illegitimate observer, data decomposition, split data transfer, Reed-Muller codes, confidentiality, polynomials of several variables, parallel communication channels.*

### *References*

1. Deundyak V.M., Mogilevskaya N.S. Skhema razdelennoj peredachi konfidentsial'nykh dannykh na osnove differentsirovaniya polinomov neskol'kikh peremennykh nad prostymi polyami Galua // Voprosy kiberbezopasnosti. 2017. №5 (24). S.64-71. DOI: 10.21681/2311-3456-2017-5-64-71.
2. Kosolapov YU.V. Metod kodovogo zashumleniya v zadachakh zashhity informatsii.-Rostov-na-Donu: YUFU, 2014. 164 s.
3. Bukashkin S.A. Metod sluchajnogo kodirovaniya // Radiotekhnika. 2014. №4. S. 31-36.
4. Fukumoto S., Wadayama T. Iterative erasure correcting algorithm for q-ary Reed-Muller codes based on local correctability. 9th International Symposium on Turbo Codes and Iterative Information Processing (ISTC IEEE). (Brest, France, 5-9 Sept., 2016). Pp. 36 – 40. DOI: 10.1109/ISTC.2016.7593072
5. Kudekar S., Kumar S., Mondelli M., Pfister H. D., Sasoglu E., Urbanke R. Reed-Muller codes achieve capacity on erasure channels. IEEE Trans. Inform. Theory, vol. 63, no. 7, pp. 4298-4316, 2017.

1 Vladimir M. Deundyak, Ph.D. (in Math.), Associate Professor, Associate Professorof at Institute of Mathematics, Mechanics and Computer Science, Southern Federal University, FSASE SRI «Specvuzavtomatika», Rostov-on-Don, Russia, E-mail: vl.deundyak@gmail.com. ORCID 0000-0001-8258-2419.

2 Nadezhda S. Mogilevskaya, Ph.D., Associate Professor, Associate Professor at Institute of Mathematics, Mechanics and Computer Science, Southern Federal University, Rostov-on-Don, Russia, E-mail: nadezhda.mogilevskaia@yandex.ru. ORCID 0000-0003-13575869.

6. Santi E., Hager C. Pfister H. Decoding Reed-Muller Codes Using Minimum-Weight Parity Checks. IEEE International Symposium on Information Theory (ISIT). 2018. Pp. 1296 – 1300.
7. Saptharishi R., Shpilka A., Volk B. L. Efficiently decoding Reed–Muller codes from random errors. Proc. 48th Annu. ACM Symp. Theory Comput. (STOC), pp. 227-235, 2016, [online] Available: http://doi.acm.org/10. 1145/2897518.2897526.
8. Young Gil Kim, A. J. Han Vinck. 4-Ary Codebook Design Using Reed–Muller Codes for MIMO Beamforming Systems. IEEE Transactions on Vehicular Technology (Vol. 65, Issue: 2, Feb. 2016). Pp. 959 – 966. DOI: 10.1109/TVT.2015.2404844
9. Kozlovskij A.V., Nasyrov A.M. Spetsifika primeneniya strukturnykh osobennostej kodovykh kombinatsij polyarnykh kodov i kodov Rida-Mallera Sovremennye problemy proektirovaniya, proizvodstva i ehkspluatatsii radiotekhnicheskikh sistem. 2017. № 1-2 (10). S. 159-161.
10. Borodin M.A., CHizhov I.V. Ehfektivnaya ataka na kriptosistemu Mak-EHlisa, postroennuyu na osnove kodov Rida-Mallera Diskretnaya matematika. 2014. T. 26. № 1. S. 10-20.
11. Deundyak V.M., Mogilevskaya N.S. Vosstanovlenie dannykh iz otvodnogo kanala nablyudeniya s ispol'zovaniem dekoderov, rabotayushhikh za predelom poloviny kodovogo rasstoyaniya // Telekommunikatsii. 2017. № 4. S. 27-33.
12. Deundyak V.M., Mogilevskaya N.S. Ob ispol'zovanii myagkikh i veroyatnostnykh dekoderov dlya vosstanovleniya dannykh pri perekhvate // Izvestiya vysshikh uchebnykh zavedenij. Severo-Kavkazskij region. Seriya: Estestvennye nauki. 2017. № 1 (193). S. 18-24.
13. Deundyak V.M., Mogilevskaya N.S. Model' troichnogo kanala peredachi dannykh s ispol'zovaniem dekodera myagkikh reshenij kodov Rida-Mallera vtorogo poryadka // Izvestiya vuzov. Severo-Kavkazskij region. Tekhnicheskie nauki, 2015. № 1. S. 3–10.
14. Deundyak V.M., Mogilevskaya N.S. Differentsirovanie polinomov neskol'kikh peremennykh nad polyami Galua nechetnoj moshhnosti i prilozheniya k kodam Rida-Mallera. Vestnik Donskogo gosudarstvennogo tekhnicheskogo universiteta. 2018. № 18(3) S. 339-348. DOI: 10.23947/1992-5980-2018-18-3-339-348
15. Deundyak V. M., Knutova A. V. Integriruemost' sistem polinomov neskol'kikh peremennykh pervoj i vtoroj stepeni nad prostymi polyami Galua // Izvestiya VUZov. Severo-Kavkazskij region. Estestvennye nauki. 2016. №2. S. 41–46.
16. Deundyak V. M., Mogilevskaya N. S. Ob usloviyakh korrektnosti dekodera myagkikh reshenij troichnykh kodov Rida-Mallera vtorogo poryadka. Vladikavkazskij matematicheskij zhurnal. 2016, T. 18. Vyp. 4. C.23-33.
17. Shnajer B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si – M.: Triumf, 2016. – 816 s.