Раздел III. Криптографическая защита информации

УДК 004.056.5

В.М. Деундяк, С.А. Евпак, В.В. Мкртичян

МОНОТОННОСТЬ РУБЕЖЕЙ В СПЕЦИАЛЬНОЙ СХЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ, ОСНОВАННОЙ НА Q-ИЧНЫХ КОДАХ РИДА-МАЛЛЕРА

Исследуется возможность применения кодовой схемы защиты легально тиражируемой цифровой продукции от несанкционированного распространения. В этой схеме каждый легальный пользователь имеет уникальный вектор ключ для доступа к данным. В случае нелегального распространения этого вектор–ключа пользователь может быть идентифицирован контролером. Однако, легальные пользователи, являющиеся злоумышленниками, могут объединяться в коалиции для создания пиратских вектор-ключей доступа к данным с целью дальнейшего их распространения без боязни быть выявленными. Схема защиты позволяет контролеру найти по обнаруженному пиратскому вектор-ключу как минимум одного из членов коалиции злоумышленников при условии, что число злоумышленников не превзошло некоторого заранее оговоренного порога $c(\in N)$, зависящего от параметров базового помехоустойчивого кода. В случае же превышения порога c при поиске злоумышленников по пиратскому вектор-ключу возможна компрометация контролером невиновного пользователя. Целью работы является исследование случая превышения порога c для дальнейшей организации выбора таких значений параметров базового кода, при которых возможность компрометации невиновных пользователей минимальна. Для достижения этой цели решаются следующие задачи. Для схемы защиты введены, области компрометации, базирующееся на Q-ичных кодах Рида-Маллера $RM_q(r,m)$. Вводится широкая область косвенной компрометации – множество таких значений c, при которых в качестве наиболее вероятного злоумышленника контролер может принять невиновного пользователя, и узкая область непосредственной компрометации – множество таких значений c, при которых в качестве единственного злоумышленника контролером может принять невиновного пользователя. Вводятся рубежи областей компрометации. Определяются численные границы рубежей областей компрометации. Обосновывается монотонность этих рубежей по параметрам r и m базового кода $RM_q(r,m)$. Для решения этих задач используются методы алгебры, теории множеств и теории помехоустойчивого кодирования. Полученные в результате решения этих задач теоретические результаты направлены на проектирование кодовых схемы защиты, гибко реагирующих на превышение допустимой мощности коалиции злоумышленников.

Q-коды Рида-Маллера; списочное декодирование; широковещательное шифрование; поиск злоумышленников.

V.M. Deundyak, V.V. Mkrtichan, S.A. Yevpak

MONOTONICITY PROPERTIES OF THE BOUNDS THE SPECIFIC INFORMATION PROTECTION SCHEME BASED ON THE *Q*-ARY REED-MULLER CODES

The purpose is to study bounds of applying of the specific information protection scheme. In the scheme every user have unique vector-key used to access distributable data. In case of its illegal publishing the user can be identified by an inspector. However malicious legal users named traitors can compose a coalitions. Coalitions can create a pirate vector-keys to illegal distribution. The scheme allow inspector to identify at least one traitor from coalition by pirate key if coalition

volume not exceeds some threshold $c(\in N)$, which depends on parameters of a base error-correction code. In case of exceeding c inspector can unintentionally compromise innocent user. The purpose is to study the case to organize base code selecting, which minimize compromising opportunity. To scheme based on q-ary Reed-Muller codes $RM_q(r,m)$ compromising domains are considered. Particularly considered wide domain of indirect compromising which is values of c that leads to opportunity to regard innocent user as high probably member of coalition and narrow domain of direct compromising which is values of c that leads to opportunity to regard the user as single member of coalition. A thresholds of the domains and its numeric bounds are considered. Monotonicity of threshold of indirect compromising domain and threshold of direct compromising domain by the r and m parameters of $RM_q(r,m)$ code are proved. The theoretical results is purported to choosing values of parameters of used q-ary Reed-Muller codes during the design of specific information protection scheme based on error correction code.

Q-ary Reed-Muller codes; list decoding; broadcast encryption; traitor tracing.

1. Введение и постановка задачи. В работах [1–3] рассмотрен перспективный способ защиты легально тиражируемой цифровой продукции от несанкционированного распространения, называемый схемой специального широковещательного шифрования (ССШШ). Данный способ основан на использовании специальных кодов защиты при наличии коалиции злоумышленников. В качестве таких кодов в работах [4, 5] предложено использовать q-ичные коды Рида-Маллера $RM_q(r,m)$. Однако в случае непредусмотренного превышения мощности коалиции в ССШШ возможна компрометация невиновного пользователя. В [6, 7] для схемы защиты на кодах Рида-Соломона описаны области компрометации и соответствующие рубежи. В [8, 9] введены их аналоги для q-ичных кодов Рида-Маллера. Данная работа является продолжением этих работ и исследует свойства монотонности рубежей по параметрам r и m.

Целью работы является исследование случая превышения порога c для дальнейшей организации выбора значений параметров базового кода, при которых возможность компрометации невиновных пользователей минимальна. Актуальность темы исследования подтверждается работами [10–19]. Доказанные результаты направлены на проектирование кодовых схем защиты, гибко реагирующих на превышение допустимой мощности коалиции злоумышленников.

2. Математическая модель схемы специального широковещательного шифрования, основанной на q-ичных кодах Рида-Маллера. Пусть $\mathbf{N}$ – множество натуральных чисел, $N_1 = \mathbf{N}\backslash\{1\}$, $\mathbf{F}_q[X_1, X_2, \dots, X_m]$ – кольцо полиномов m переменных с коэффициентами из поля Галуа $\mathbf{F}_q$**.** Под q-ичным кодом Рида-Маллера $RM_q(r,m)$ порядка r будем понимать аналогично [20] множество векторов длины $n = q^m$ вида $(f(\boldsymbol{P}_1), f(\boldsymbol{P}_2), \dots, f(\boldsymbol{P}_n))$, где f пробегает все подпространство полиномов $\mathbf{F}_q^r[X_1, \dots, X_m]$ степени не выше r кольца $\mathbf{F}_q[X_1, X_2, \dots, X_m]$, а $\boldsymbol{P}_1, \boldsymbol{P}_2, \dots, \boldsymbol{P}_n$ – фиксированное упорядочение элементов пространства Хемминга $\mathbf{F}_q^m = \mathbf{F}_q \times \dots \times \mathbf{F}_q$.

Под степенью монома $X_1^{t_1} X_2^{t_2} \dots X_m^{t_m} \in (\mathbf{F}_q[X_1, X_2, \dots, X_m])$ понимается натуральное число $\sum_{i=1}^{m} t_i$, а под степенью полинома f из $\mathbf{F}_q[X_1, X_2, \dots, X_m]$ – максимальная из степеней входящих в него мономов.

Рассмотрим схему специального широковещательного шифрования (ССШШ), основанную на q-ичных кодах Рида-Маллера. Защищаемые данные тиражируются свободно в зашифрованном виде, а каждому легальному пользователю выдается уникальная ключевая пара и, в частности, так называемый вектор-номер, являющийся словом помехоустойчивого кода $RM_q(r,m)$ и необходимый для получения доступа к распространяемым данным в ССШШ. В случае обнаружения нелегального использования такой пары ее хозяин может быть идентифицирован контролером (см. [2, 4, 6, 7].

Однако злоумышленники могут объединить свои вектор-номера в коалицию и строить потомков коалиции. Множество всевозможных коалиций кода C мощности не более $c(\geq 2)$ обозначается аналогично [8] через $\mathrm{coal}_c(C)$; множество потомков коалиции $C_0 \in \mathrm{coal}_c(C)$ обозначается через $\mathrm{desc}(C_0)$ и определяется правилом:

$$\mathrm{desc}(C_0) = \{w = (w_1, \dots, w_n) \in \mathbf{F}_q^n : \forall i \in \{1; \dots; n\}\ w_i \in C_{0,i}\},$$

где $C_{0,i}$ – множество i-х координат всех вектор-номеров коалиции C_0; множество пиратских вектор-номеров коалиции C_0 определяется правилом $\mathrm{desc}(C_0) \backslash C_0$. Под множеством-потомков кода C будем понимать

$$\mathrm{desc}_c(C) = \bigcup_{C_i \in \mathrm{coal}_c(C)} \mathrm{desc}(C_i).$$

Пиратские вектор-номера можно применять для нелегального доступа к тиражируемым данным (см., например, [4], [6]).

Для защиты от такого рода коалиционных атак в [2] предложен метод, основанный на применении в ССШШ специальных кодов защиты от копирования и списочного декодирования этих кодов, с помощью которого контролер может идентифицировать по пиратскому вектор-номеру членов создавшей его коалиции. В работе [20] представлен один из алгоритмов списочного декодирования q-ичного кода Рида-Маллера с управляющими параметрами q, r и m. Алгоритм действий контролера описан в [4]. Метод исходит из предположения, что максимально возможное количество злоумышленников не превосходит некоторого числа $c(\geq 2)$, и опирается на описанных ниже классах кодов.

Пусть $c \in N_1$, C – произвольный код. Код C является c-FP-кодом тогда и только тогда, когда

$$\forall C_0 \in \mathrm{coal}_c(C)\ \forall z \in C:\ z \in \{C \backslash C_0\} \Rightarrow z \notin \mathrm{desc}(C_0) \backslash C_0.$$

Пусть $c \in N_1$, C – произвольный код. Код C является c-TA-кодом тогда и только тогда, когда

$$\forall C_0 \in \mathrm{coal}_c(C) \forall w \in \mathrm{desc}(C_0) \forall z \in C \backslash C_0 \exists y \in C_0 : d(w, y) \leq d(w, z).$$

Отметим, что код C является c-TA-кодом тогда и только тогда, когда для любого пиратского вектор-номера $w \in \mathrm{desc}_c(C)$ ближайшим кодовым словом является элемент y, входящий в каждую из создающих его коалиций. Этот элемент в [6] предлагается находить переборным декодером. Кроме того, если код C является c-TA-кодом, то код C является c-FP-кодом. В [5] доказано, что если для параметров кода $RM_q(r, m)$ выполняется условие $r < q$, и

$$c \leq B_0\big(RM_q(r, m)\big) = \left\lfloor \sqrt{\frac{q}{r}} \right\rfloor, \quad (1)$$

то код $RM_q(r, m)$ является c-TA-кодом.

Рассмотрим q-ичный код Рида-Маллера $RM_q(r, m)$ с параметрами такими, что выполняется условие (1). Тогда код $RM_q(r, m)$ является c-TA-кодом и может быть использован для защиты от коалиционных атак [4]. При этом при обнаружении пиратского вектор-номера w применяется следующий порядок действий контролера в эффективной ССШШ: подать q, r и m и вектор w на вход списочному декодеру (см. [20]) и на выходе получить список $b(\subseteq C)$ легальных вектор-номеров из коалиции. Из того, что c-TA-коды являются и c-FP-кодами, следует, что помимо возможности эффективного поиска злоумышленников в модели исключается возможность прямой компрометации невиновных пользователей. Под компрометацией пользователя контролером будем понимать существование такого потомка из $\mathrm{desc}_c(C)$, что применение к нему декодера дает список, включающий вектор-номер данного пользователя.

3. Схема специального широковещательного шифрования, основанная на q-ичных кодах Рида-Маллера, в случае превышения пороговой мощности коалиции. Рассмотрим схему защиты, представленную в разделе 2. Условие $c \le B_0\left(RM_q(r,m)\right)$ является необходимым условием корректной работы эффективной ССШШ. При превышении мощности коалиции порога $B_0\left(RM_q(r,m)\right)$ корректная работа модели не гарантируется. Аналогично [8] далее будем рассматривать следующие возможные результаты работы контролера при обнаружении пиратского вектор-номера $w \in \mathrm{desc}_c(C)$, этой ситуации:

1. В результате применения списочного декодера контролером ближайшим к w оказывается вектор-номер невиновного пользователя. Это событие назовем компрометацией невиновного пользователя списочным декодером. При этом контролер имеет возможность проанализировать список вектор-номеров, в котором в качестве вектор-номера злоумышленника имеет смысл рассматривать вектор-номер, ближайший к w.

2. Вектор-номер w легальный, но создан некоторой коалицией ($w \in \mathrm{desc}_c(C) \cap C$). Это событие назовем прямой компрометацией невиновного пользователя. При этом контролер не имеет возможности обнаружить факт коалиционной атаки.

По аналогии с [8] введем множества $\Omega_{TA;r,m}$ и $\Omega_{FP;r,m}$, которые будем называть областями компрометации кода $RM_q(r,m)$. Пусть

$$\Omega_{TA;r,m} = \{c \in N_1 : \exists v \in RM_q(r,m)\ \exists C_0 \in \mathrm{coal_c}\left(RM_q(r,m)\backslash\{v\}\right) \exists w \in \mathrm{desc}(C_0)\backslash C_0\ \forall u \in C_0 : d(w,v) \le d(w,u)\}.$$

Область $\Omega_{TA;r,m}$ кода $RM_q(r,m)$ есть множество мощностей таких коалиций, при которых для некоторого кодового слова v существует коалиция C_0 этой мощности, у которой хотя бы один из потомков расположен не далее v, чем от любого элемента C_0. Очевидно, что $\Omega_{TA;r,m}$ – множество таких значений $c \in N_1$, для которых кода $RM_q(r,m)$ не является c-TA-кодом. Область $\Omega_{TA;r,m}$ кода $RM_q(r,m)$ представляет собой множество мощностей таких коалиций, при которых результатом работы контролера будет случай 1.

Пусть

$$\Omega_{FP;r,m} = \{c \in N_1 : \exists v \in RM_q(r,m)\ \exists C_0 \in \mathrm{coal_c}\left(RM_q(r,m)\backslash\{v\}\right) : v \in \mathrm{desc}(C_0)\backslash C_0\}.$$

Область $\Omega_{FP;r,m}$ кода $RM_q(r,m)$ есть множество мощностей таких коалиций, при которых для некоторого кодового слова v существует коалиция, у которой v является потомком. Очевидно, что $\Omega_{FP;r,m}$ – множество таких значений $c \in N_1$, для которых кода $RM_q(r,m)$ не является c-FP-кодом. Область $\Omega_{FP;r,m}$ кода $RM_q(r,m)$ представляет собой множество мощностей таких коалиций, при которых результатом работы контролера будет случай 2.

Очевидно, $\Omega_{TA;r,m}$ и $\Omega_{FP;r,m}$ – целочисленные отрезки вида:

$$\Omega_{TA;r,m} = \{R_{TA}(r,m); \dots; |RM_q(r,m)|\},$$
$$\Omega_{FP;r,m} = \{R_{FP}(r,m); \dots; |RM_q(r,m)|\},$$

где $R_{TA}(r,m)$ и $R_{FP}(r,m)$– величины, которые будем называть рубежами областей компрометации $\Omega_{TA;r,m}$ и $\Omega_{FP;r,m}$ соответственно.

Интерес представляет собой задача вычисления мощности областей компрометации, которая сводится к задаче расчета рубежей $R_{TA}(r,m)$ и $R_{FP}(r,m)$ или, в случае неудачи, к задаче получения границ для значений $R_{TA}(r,m)$ и $R_{FP}(r,m)$. Непосредственно из определений вытекает справедливость вложения $\Omega_{FP;r,m} \subseteq \Omega_{TA;r,m}$, и, следовательно,

$$R_{TA}(r,m) \le R_{FP}(r,m).$$

Кроме того, из определения $\Omega_{TA;r,m}$ и неравенства (1) следует, что

$$B_0\left(RM_q(r,m)\right) \le R_{TA}(r,m).$$

Теорема 1. Если $\left\lfloor \frac{(q^m-q+1)^2}{q^{2m-1}}+1 \right\rfloor \le r < q$, то $R_{TA}(r,m) \le \left\lceil \sqrt{\frac{q}{r}} \right\rceil$. Если $r < q$ и $r < \left\lfloor \frac{(q^m-q+1)^2}{q^{2m-1}}+1 \right\rfloor$, то $R_{TA}(r,m) \le \left\lfloor \frac{q}{r}+1-\frac{1}{rq^{m-2}}+\frac{1}{rq^{m-1}} \right\rfloor$. Если $r < q$, то $R_{FP}(r,m) = \left\lceil \frac{q}{r} \right\rceil$.

Доказательство теоремы 1 основано на громоздких комбинаторных вычислениях, использует результаты работ [5], [8], [9], [19] и публикуется отдельно.

Ниже представлены свойства монотонности рубежей $R_{TA}(r,m)$ и $R_{FP}(r,m)$ по параметрам r и m кода $RM_q(r,m)$.

4. Результаты монотонности рубежей $R_{TA}(r,m)$ и $R_{FP}(r,m)$. Сначала рассмотрим монотонность рубежа $R_{TA}(r,m)$.

Теорема 2. Пусть r_1, r_2, $m \in \mathbf{N}$, а $C^1 = RM_q(r_1,m)$ и $C^2 = RM_q(r_2,m)$ – q-ичные коды Рида-Маллера. Если выполняется условие $r_1 < r_2$, то для рубежей $R_{TA}(r_1,m)$ и $R_{TA}(r_2,m)$ выполняется неравенство

$$R_{TA}(r_1,m) \ge R_{TA}(r_2,m).$$

Доказательство. Так как $r_1 < r_2$, то имеет место вложение $\mathbf{F}_q^{r_1}[X_1,\dots,X_m] \subset \mathbf{F}_q^{r_2}[X_1,\dots,X_m]$, и, следовательно, и вложение $C^1 \subset C^2$. Пусть $c \in N_1$ – такое, что выполняется условие

$$\exists v_1 \in C^1\ \exists C_1 \in \mathrm{coal_c}(C^1 \backslash \{v_1\})\ \exists w_1 \in \mathrm{desc}(C_1) \backslash C_1 \forall u \in C_1: \\ d(v_1,w_1) \le d(w_1,u).$$

Тогда ввиду условия $C^1 \subset C^2$ выполняется условие

$$\exists v_2 (\in C^2) = v_1\ \exists C_2 \in \mathrm{coal_c}(C^2 \backslash \{v_2\}) = C_1\ \exists w_2 (\in \mathrm{desc}(C_2) \backslash C_2) = w_1 \\ \forall u \in C_2 \colon d(v_2,w_2) \le d(w_2,u).$$

По определению $\Omega_{TA;r,m}$ имеет место вложение $\Omega_{TA;r_1,m} \subseteq \Omega_{TA;r_2,m}$, а, значит, неравенство $R_{TA}(r_1,m) \ge R_{TA}(r_2,m)$ выполняется. ■

Теорема 3. Пусть r, m_1, $m_2 \in \mathbf{N}$, а $C^1 = RM_q(r,m_1)$ и $C^2 = RM_q(r,m_2)$ – q-ичные коды Рида-Маллера. Если выполняется условие $m_1 < m_2$, то для рубежей $R_{TA}(r,m_1)$ и $R_{TA}(r,m_2)$ выполняется неравенство

$$R_{TA}(r,m_1) \ge R_{TA}(r,m_2).$$

Доказательство. Пусть $\varphi_1 \colon \mathbf{F}_q^r[X_1, X_2 \dots, X_{m_1}] \to \mathbf{F}_q^{n_1}$ – кодирующее отображение кода C^1, то есть

$$\varphi_1(f) = \big(f(\boldsymbol{P}_1), f(\boldsymbol{P}_2), \dots, f(\boldsymbol{P}_{n_1})\big),$$

где поле Галуа $\mathbf{F}_q$ состоит из элементов $\alpha_1, \alpha_2, \dots, \alpha_q$, $n_1 = q^{m_1}$, а точки $\boldsymbol{P}_1, \boldsymbol{P}_2, \dots, \boldsymbol{P}_{n_1} (\in \mathbf{F}_q^{m_1})$ имеют вид $\boldsymbol{P}_1 = (\alpha_1, \alpha_1, \dots, \alpha_1, \alpha_1)$, $\boldsymbol{P}_2 = (\alpha_1, \alpha_1, \dots, \alpha_1, \alpha_2)$, $\boldsymbol{P}_3 = (\alpha_1, \alpha_1, \dots, \alpha_1, \alpha_3)$, …, $\boldsymbol{P}_{n_1} = (\alpha_q, \alpha_q, \dots, \alpha_q, \alpha_q)$.

Для доказательства теоремы достаточно показать, что неравенство $R_{TA}(r,m_1) \ge R_{TA}(r,m_2)$ выполняется для $m_2 = m_1 + 1$. Пусть $m_2 = m_1 + 1$ и пусть $\varphi_2 \colon \mathbf{F}_q^r[X_1, X_2 \dots, X_{m_2}] \to \mathbf{F}_q^{n_2}$ – кодирующее отображение кода C^2, т.е.

$$\varphi_2(f) = (f(\boldsymbol{Q}_1), f(\boldsymbol{Q}_2), \dots, f(\boldsymbol{Q}_{n_2})),$$

где $n_2 = q^{m_2}$, а точки $\boldsymbol{Q}_1, \boldsymbol{Q}_2, \dots, \boldsymbol{Q}_{n_2} (\in \mathbf{F}_q^{m_2})$, имеют вид

$$\boldsymbol{Q}_{in_1} = (Z(i), \alpha_1, \alpha_1, \dots, \alpha_1, \alpha_1),\ \boldsymbol{Q}_{in_1+1} = (Z(i), \alpha_1, \alpha_1, \dots, \alpha_1, \alpha_2), \dots, \\ \boldsymbol{Q}_{in_1+n_1-1} = \big(Z(i), \alpha_q, \alpha_q, \dots, \alpha_q, \alpha_q\big),$$

где $i \in \{1; \dots; q\}$, $Z(i) = \alpha_i$.

Пусть $f \in \mathbf{F}_q^r[X_1, X_2 \dots, X_{m_1}]$, тогда $f \in \mathbf{F}_q^r[X_1, X_2 \dots, X_{m_2}]$, при этом

$$\varphi_2(f) = (f(\boldsymbol{Q}_1), f(\boldsymbol{Q}_2), \dots, f(\boldsymbol{Q}_{n_2})) = (\varphi_1(f), \dots, \varphi_1(f)).$$

Пусть $v(\in C^1) = (v_1, \dots, v_{n_1})$ – произвольное кодовое слово, а $f_v \in$ $\mathbf{F}qrX1,X2\dots,Xm1$ – многочлен, такой, что $\varphi 1 f v = v$. Тогда

$$\varphi_2(f_v) = (v'_1, \dots, v'_{qn_1}) = (v_1, \dots, v_{n_1}, \dots, v_1, \dots, v_{n_1}, \dots, v_1, \dots, v_{n_1}).$$

Пусть $c \in \Omega_{TA;r,m_1}$.

Рассмотрим многочлен $f_{v_1} \in \mathbf{F}_q^r[X_1, X_2 \dots, X_{m_1}]$, такой, что $\varphi_1(f_{v_1}) = v_1$

$$v_2(\in C^2) = \varphi_2(f_{v_1}) = (v_{1,1}, \dots, v_{1,n_1}, \dots, v_{1,1}, \dots, v_{1,n_1}).$$

Рассмотрим также коалицию

$$C_2(\in \mathrm{coal_c}(C^2 \backslash \{v_2\})) = \{\varphi_2(f(u_1)); \dots; \varphi_2(f(u_c))\},$$

где $f_{u_i} \in \mathbf{F}_q^r[X_1, X_2 \dots, X_{m_2}]$ – многочлены, такие, что $\varphi_2(f(u_i)) = u_i$, а $i \in \{1; \dots; c\}$. Пусть $w_2 (\in \mathbf{F}_q^{n_2}) = (w_1, \dots, w_{n_1}, \dots, w_1, \dots, w_{n_1})$. Тогда $w_2 \in \mathrm{desc}(C_2)$. Кроме того

$$\forall u_i \in C_2 \colon d(v_2, w_2) \leq d(w_2, u_i).$$

По определению $\Omega_{TA;r,m_2}$ выполняется условие $c \in \Omega_{TA;r,m_2}$. Значит, если $c \in \Omega_{TA;r,m_1}$, то и $c \in \Omega_{TA;r,m_2}$. Таким образом, неравенство

$$R_{TA}(r, m_1) \geq R_{TA}(r, m_2)$$

выполняется. ■

Ниже приведем прямое доказательство монотонности рубежа $R_{FP}(r, m)$ по первому параметру.

Теорема 4. Пусть r_1, r_2, $m \in \mathbf{N}$, а $C^1 = RM_q(r_1, m)$ и $C^2 = RM_q(r_2, m)$ – q-ичные коды Рида-Маллера. Если выполняется условие $r_1 < r_2$, то для рубежей $R_{FP}(r_1, m)$ и $R_{FP}(r_2, m)$ выполняется неравенство

$$R_{FP}(r_1, m) \geq R_{FP}(r_2, m).$$

Доказательство. Так как $r_1 < r_2$, то имеет место вложение $\mathbf{F}_q^{r_1}[X_1, \dots, X_m] \subset \mathbf{F}_q^{r_2}[X_1, \dots, X_m]$, и, следовательно, и вложения $C^1 \subset C^2$. Пусть $c \in N_1$ – такое, что выполняется условие

$$\exists v_1 \in C^1 \; \exists C_1 \in \mathrm{coal_c}(C^1 \backslash \{v_1\}) \colon v_1 \in \mathrm{desc}(C_1) \backslash C_1.$$

Тогда ввиду условия $C^1 \subset C^2$ выполняется условие

$\exists v_2 (\in C^2) = v_1 \; \exists C_2 \in \mathrm{coal_c}(C^2 \backslash \{v_2\}) = C_1 \colon v_2 \in \mathrm{desc}(C_2) \backslash C_2$.

По определению $\Omega_{FP;r,m}$ имеет место вложение $\Omega_{FP;r_1,m} \subseteq \Omega_{FP;r_2,m}$, а, значит, неравенство

$$R_{FP}(r_1, m) \geq R_{FP}(r_2, m)$$

выполняется. ■

Полученные теоретические результаты можно использовать в ходе проектирования ССШШ при выборе значений параметров r, m, q применяемого в ССШШ q-ичного кода Рида-Маллера.

Заключение. Целью работы является исследование случая превышения порога c для дальнейшей организации выбора значений параметров базового кода, при которых возможность компрометации невиновных пользователей минимальна. В работе доказаны теоретические результаты, направленные на проектирование кодовых схем защиты, являющихся безопасными в указанном отношении.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Кабатянский Г.А.* Коды защиты от копирования: случай двух пиратов // Проблемы передачи информации. – 2005. – Т. 41, № 2. – С. 123-127.
2. *Silverberg A., Staddon J., Walker J.* Application of list decoding to tracing traitors // In Adv. in Crypt. – ASIACRYPT 2001 (LNCS 2248). – 2001. – P. 175-192.
3. *Staddon J.N., Stinson D.R., Wei R.* Combinatorial properties of frameproof and traceability codes // IEEE Trans. On Inf. Theory. – 2001. – Vol. 47. – P. 1042-1049.

4. *Евпак С.А., Мкртичян В.В.* Применение *q*-ичных кодов Рида-Маллера в схемах специального широковещательного шифрования // Труды научной школы И.Б. Симоненко. – 2010. – С. 93-99.
5. *Евпак С.А., Мкртичян В.В.* Исследование возможности применения *q*-ичных кодов Рида-Маллера в схемах специального широковещательного шифрования // Известия вузов. Северо-Кавказский регион. Естественные науки. – 2011. – № 5. – С. 11-15.
6. *Деундяк В.М., Мкртичян В.В.* Математическая модель эффективной схемы специального широковещательного шифрования и исследование границ ее применения // Известия вузов. Северо-Кавказский регион. Естественные науки. – 2009. – № 1. – С. 5-8.
7. *Деундяк В.М., Мкртичян В.В.* Исследование границ применения схемы защиты информации, основанной на РС-кодах // Дискретный анализ и исследование операций. – 2011. – Т. 18, № 1. – С. 21-38.
8. *Евпак С.А., Мкртичян В.В.* О связи границ применения специальной схемы защиты информации, основанной на *q*-ичных кодах Рида-Маллера // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 194-200.
9. *Евпак С.А., Мкртичян В.В.* Условия применения *q*-ичных кодов Рида-Маллера в специальных схемах защиты информации от несанкционированного доступа // Владикавказский математический журнал. – 2014. – Т. 16, № 2. – С. 27-34.
10. *Anthapadmanabhan N., Barg A.* Two-level Fingerprinting: Stronger definitions and code constructions // in Proc. IEEE Int. Symp. Inform. Theory (ISIT), Austin, TX. – 2010. – P. 2528-2532.
11. *Barg A., Blakley G.R. and Kabatiansky G*. Digital fingerprinting codes: problem statements, constructions, identification of traitors // IEEE Trans. on Information Theory. – 2003. – Vol. 49. – P. 852-865.
12. *Fernandez M., Cotrina J., Soriano M., and N. Domingo.* A note about the identifier parent property in Reed-Solomon codes // Comput. Security. – 2010. – Vol. 20, No. 5. – P. 628-635.
13. *Fernandez M., Moreira J., and Soriano M.* Identifying traitors using the Koetter-Vardy algorithm // IEEE Trans. Inf. Th. – 2011. – Vol. 57, No. 2. – P. 692-704.
14. *Jin H., Blaum M.* Combinatorial properties for traceability codes using error correcting codes // IEEE Trans. Inf. Theory. – 2007. – Vol. 53, No. 2. – P. 804-808.
15. *Moreira J., Fernandez M., and Kabatiansky G.* Constructions of almost secureframeproof codes based on small-bias probability spaces // in Proc. Int. Workshop Security (IWSEC), (LNCS 8231), Okinawa, Japan. – 2013. – P. 53-67.
16. *Moreira J., Fernandez M., and Soriano M*. On the relationship between the traceability properties of Reed-Solomon codes // Adv. Math. Commun. – 2012. – Vol. 6, No. 4. – P. 467-478.
17. *Moreira J., Fernandez M., and Soriano M.* Propiedades de trazabilidad de los codigos de Reed-Solomon para ciertos tama~nos de coalicion // in Proc. Reunion Espanola sobre Criptologa y Seguridad de la Informacion (RECSI), Tarragona, Spain. – 2010. – P. 413-417.
18. *Moreira J., Kabatiansky G., and Fernandez M*. Lower bounds on almostseparating binary codes // in Proc. IEEE Int. Workshop Inform. Forensics, Security (WIFS), Foz do Iguacu, Brazil. – 2011. – P. 1-6.
19. *Fernandez M., Cotrina J., Sorario M. and Domingo N.* A note about the traceability properties of linear codes // In Information Security and Cryptology – ICISC 2007 (LNCS 4817). – 2007. – P. 251-258.
20. *Pellikaan R., Wu X.-W*. List decoding of *q*-ary Reed-Muller Codes // IEEE Trans. On Information Theory. – 2004. – Vol. 50, № 4. – P. 679-682.

REFERENCES

1. *Kabatyanskiy G.A.* Kody zashchity ot kopirovaniya: sluchay dvukh piratov [Codes copy protection: the case of two pirates], *Problemy peredachi informatsii* [Problems of information transmission], 2005, Vol. 41, No. 2, pp. 123-127.
2. *Silverberg A., Staddon J., Walker J.* Application of list decoding to tracing traitors, *In Adv. in Crypt. ASIACRYPT 2001 (LNCS 2248)*, 2001, pp. 175-192.
3. *Staddon J.N., Stinson D.R., Wei R.* Combinatorial properties of frameproof and traceability codes, *IEEE Trans. On Inf. Theor*y, 2001, Vol. 47, pp. 1042-1049.

4. *Evpak S.A., Mkrtichyan V.V.* Primenenie q-ichnykh kodov Rida-Mallera v skhemakh spetsial'nogo shirokoveshchatel'nogo shifrovaniya [The application of q-ary reed-Muller codes in the special schemes for broadcast encryption], *Trudy nauchnoy shkoly I.B. Simonenko* [Proceedings of the scientific school of I.B. Simonenko], 2010, pp. 93-99.
5. *Evpak S.A., Mkrtichyan V.V.* Issledovanie vozmozhnosti primeneniya q-ichnykh kodov Rida-Mallera v skhemakh spetsial'nogo shirokoveshchatel'nogo shifrovaniya [Research of possibility of application of q-ary reed-Muller codes in the special schemes for broadcast encryption], *Izvestiya vuzov. Severo-Kavkazskiy region. Estestvennye nauki* [Izvestiya vuzov. Severo-kavkazskii region. Natural sciences], 2011, No. 5, pp. 11-15.
6. *Deundyak V.M., Mkrtichyan V.V.* Matematicheskaya model' effektivnoy skhemy spetsial'nogo shirokoveshchatel'nogo shifrovaniya i issledovanie granits ee primeneniya [A mathematical model of effective special schemes for broadcast encryption and a study of the boundaries of its application], *Izvestiya vuzov. Severo-Kavkazskiy region. Estestvennye nauki* [Izvestiya vuzov. Severo-kavkazskii region. Natural sciences], 2009, No. 1, pp. 5-8.
7. *Deundyak V.M., Mkrtichyan V.V.* Issledovanie granits primeneniya skhemy zashchity informatsii, osnovannoy na RS-kodakh [A study of the boundaries of application of the protection circuit information based on RS codes], *Diskretnyy analiz i issledovanie operatsiy* [Diskretnyi Analiz i Issledovanie Operatsii], 2011, Vol. 18, No. 1, pp. 21-38.
8. *Evpak S.A., Mkrtichyan V.V.* O svyazi granits primeneniya spetsial'noy skhemy zashchity informatsii, osnovannoy na q-ichnykh kodakh Rida-Mallera [About the link between the bounds of applying of the special information protection scheme based on the q-ary reed–muller codes], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2013, No. 12 (149), pp. 194-200.
9. *Evpak S.A., Mkrtichyan V.V.* Usloviya primeneniya q-ichnykh kodov Rida-Mallera v spetsial'nykh skhemakh zashchity informatsii ot nesanktsionirovannogo dostupa [The conditions of application of q-ary reed-Muller codes in special schemes to protect information from unauthorized access], *Vladikavkazskiy matematicheskiy zhurnal* [Vladikakazian mathematical journal], 2014, Vol. 16, No. 2, pp. 27-34.
10. *Anthapadmanabhan N., Barg A.* Two-level Fingerprinting: Stronger definitions and code constructions, *in Proc. IEEE Int. Symp. Inform. Theory (ISIT), Austin, TX,* 2010, pp. 2528-2532.
11. *Barg A., Blakley G.R. and Kabatiansky G.* Digital fingerprinting codes: problem statements, constructions, identification of traitors, *IEEE Trans. on Information Theory,* 2003, Vol. 49, pp. 852-865.
12. *Fernandez M., Cotrina J., Soriano M., and N. Domingo.* A note about the identifier parent property in Reed-Solomon codes, *Comput. Security,* 2010, Vol. 20, No. 5, pp. 628-635.
13. *Fernandez M., Moreira J., and Soriano M.* Identifying traitors using the Koetter-Vardy algorithm, *IEEE Trans. Inf. Th*., 2011, Vol. 57, No. 2, pp. 692-704.
14. *Jin H., Blaum M.* Combinatorial properties for traceability codes using error correcting codes, *IEEE Trans. Inf. Theory,* 2007, Vol. 53, No. 2, pp. 804-808.
15. *Moreira J., Fernandez M., and Kabatiansky G.* Constructions of almost secureframeproof codes based on small-bias probability spaces, in *Proc. Int. Workshop Security (IWSEC), (LNCS 8231), Okinawa, Japan,* 2013, pp. 53-67.
16. *Moreira J., Fernandez M., and Soriano M*. On the relationship between the traceability properties of Reed-Solomon codes, *Adv. Math. Commun*., 2012, Vol. 6, No. 4, pp. 467-478.
17. *Moreira J., Fernandez M., and Soriano M.* Propiedades de trazabilidad de los codigos de Reed-Solomon para ciertos tama~nos de coalicion, *in Proc. Reunion Espanola sobre Criptologa y Seguridad de la Informacion (RECSI), Tarragona, Spain*., 2010, pp. 413-417.
18. *Moreira J., Kabatiansky G., and Fernandez M*. Lower bounds on almostseparating binary codes, *in Proc. IEEE Int. Workshop Inform. Forensics, Security (WIFS), Foz do Iguacu, Brazil.* 2011, pp. 1-6.
19. *Fernandez M., Cotrina J., Sorario M. and Domingo N.* A note about the traceability properties of linear codes, *In Information Security and Cryptology – ICISC 2007 (LNCS 4817),* 2007, pp. 251-258.
20. *Pellikaan R., Wu X.-W*. List decoding of *q*-ary Reed-Muller Codes, *IEEE Trans. On Information Theory,* 2004, Vol. 50, No. 4, pp. 679-682.

Статью рекомендовала к опубликованию к.т.н. Н.С. Могилевская.

Деундяк Владимир Михайлович – Южный федеральный университет; e-mail: vl.deundyak@gmail.com; 344090, г. Ростов-на-Дону, ул. Мильчакова, 8а; тел.: +79888929337; кафедра алгебры и дискретной математики; доцент.

Евпак Сергей Александрович – e-mail: sergej-evpak@yandex.ru; тел.: +79094142919; кафедра алгебры и дискретной математики; аспирант.

Мкртичян Вячеслав Виталиевич – e-mail: realdeal@bk.ru; тел.: 89044417791; кафедра алгебры и дискретной математики; доцент.

Deundyak Vladimir Mihailovich – Southern Federal University; e-mail: vl.deundyak@gmail.com; 8a, Milchinkova street, Rostov-on-Don, 344090, Russia; phone: +79888929337; the department of algebra and discrete mathematics; associate professor.

Yevpak Sergey Alexandrovich – e-mail: sergej-evpak@yandex.ru; phone: +79094142919; the department of algebra and discrete mathematics; postgraduate student.

Mkrtichan Vyacheslav Vitalievich – e-mail: realdeal@bk.ru; phone: +79044417791; the department of algebra and discrete mathematics; associate professor.

УДК 004.056

С.В. Савин, О.А. Финько

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДАННЫХ ПОДСИСТЕМЫ РЕГИСТРАЦИИ И УЧЕТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ОСНОВЕ МЕТОДА «ОДНОКРАТНОЙ ЗАПИСИ»

Решается задача повышения защищенности хранения записей данных в подсистеме регистрации и учета системы защиты информации автоматизированной системы. Актуальность решения данной задачи заключается в необходимости защиты информации от преднамеренного воздействия со стороны легальных пользователей, которые могут скрыть следы ранее реализованных деструктивных воздействий, усиливая тем самым их вредоносный эффект или предотвращая наступление юридической ответственности за совершенные ошибочные или неправомерные действия. Предложена новая методика применения электронной подписи (или криптографической хэш-функции). При этом в общем виде реализуется известный метод так называемой «однократной записи». Однако, в отличие от известных методик, в статье предлагается структурированная методика применения электронной подписи, учитывающая такие параметры, как: глубина вложенности электронной подписи в защищаемом блоке данных (записи), количество используемых при этом криптографических ключей и порядок их использования. Порядок применения подписей – есть своеобразный ключ. Электронная подпись может быть различной – простой или усиленной (квалифицированной или неквалифицированной). Вместо подписи предусматривается применение криптографических ключевых хэш-функций. Порядок применения ключей – децентрализованный (системная подпись, подпись администратора и подписи заданного (в общем случае динамически изменяющегося) количества идентифицированных пользователей). Конкретная схема использования системы подписей может представлять собой некоторый «пространственный ключ» шифрования порядка использования упомянутых пользователей. Варьируя таким образом параметрами применения подписей и их составом, методика позволяет решать задачи защиты данных подсистемы регистрации и учета в широком диапазоне требований технического задания заказчика.

Система защиты информации; подсистема регистрации и учета; защита данных; целостность информации; метод «однократной записи»; электронная подпись.