ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 55 **2019** **Вып. 3**

УДК 621.391.15

© 2019 г. **Е.Е. Егорова**

ОБОБЩЕНИЕ IPP-КОДОВ И IPP-СИСТЕМ МНОЖЕСТВ

Четверть века назад Шор, Фиат и Наор предложили математические модели поиска источника нелегальной перепродажи цифрового контента (поиск предателей) в рамках широковещательного шифрования, в том числе следующие две комбинаторные модели: недвоичные IPP-коды на основе пороговой (n, n)-схемы разделения секрета и IPP-системы множеств на основе общей пороговой (w, n)-схемы разделения секрета. Предлагается новая схема, сочетающая в себе основные идеи IPP-кодов и IPP-систем множеств, которая может также рассматриваться как обобщение недвоичных IPP-кодов на случай равновесных кодов. В простейшем случае коалиций из двух участников дано сравнение новой схемы с ранее известными.

Ключевые слова: IPP-коды, IPP-системы множеств, схемы разделения секрета, широковещательное шифрование, равновесные коды.

DOI: 10.1134/S0555292319030045

§ 1. Постановка задачи

В работе [1] была предложена следующая модель защиты авторских прав на цифровой контент от коалиционных атак недобросовестных пользователей, называемых в [1] предателями (traitors), а соответствующие схемы – схемами поиска предателей (*ПП-схемами*). Имеется дистрибьютор, который продает доступ (в виде специального декодера) к некоторому цифровому контенту, распространяемому широковещательно. Основная проблема такого распространения данных заключается в том, чтобы сделать его устойчивым к коалиционным атакам, т.е. для любого неавторизованного декодера (пиратской версии) дистрибьютор может безошибочно идентифицировать по крайней мере одного участника из коалиции недобросовестных пользователей, создавшей этот декодер. Это свойство позднее стали называть свойством идентификации “родителей” [2] – Identifiable Parent Property (IPP).

Наиболее известными и изученными комбинаторными ПП-схемами являются IPP-коды [2] и IPP-системы множеств [3, 4]. Основная идея, лежащая в основе этих схем, была предложена в [1] и заключается в использовании пороговых совершенных схем разделения секрета [5, 6].

Пороговая (w, n)-схема “делит” секрет (“суперключ”) $k \in \mathcal{K}$, где $\mathcal{K}$ – некоторый конечный алфавит из K элементов, на n “долей” $k_1, \ldots, k_n \in \mathcal{K}$ таким образом, что любые w долей позволяют однозначно найти секрет k, в то время как меньшее число долей не дает никакой апостериорной информации о k. Схемы с последним свойством называются совершенными. Терминологию и основные свойства схем разделения секрета см. в [7, 8].

Простейшим примером совершенной схемы разделения секрета является пороговая (n, n)-схема, задаваемая соотношением

$$k_1 + \ldots + k_n = k \pmod{K}, \tag{1}$$

где $k_1, \ldots, k_{n-1}$ – случайные независимые равномерно распределенные на $\mathcal{K} = \mathbb{Z}_K$ величины.

Отметим, что t-IPP-код длины n основан на пороговой (n, n)-схеме разделения секрета, тогда как t-IPP-системы множеств основаны на использовании общей пороговой (w, n)-схемы. Семейство $\boldsymbol{F} = \{F_1, \ldots, F_M\}$, состоящее из некоторых w-подмножеств множества $\{1, \ldots, n\}$, называется t-IPP-системой множеств, если по любому w-подмножеству, принадлежащему объединению каких-то t множеств из $\boldsymbol{F}$, может быть однозначно определено хотя бы одно из этих множеств. В настоящей статье мы обобщаем понятие t-IPP-системы множеств таким образом, что как t-IPP-коды, так и t-IPP-системы множеств становятся частными случаями новой схемы поиска предателей. Неформально говоря, новая система получается "раскрашиванием" точек множества $[n] := \{1, \ldots, n\}$ в q цветов. Иначе говоря, новая ПП-схема представляет собой q-ичные коды постоянного веса с IPP-свойством, обобщающим известное свойство дизъюнктивных кодов [9,10], также называемых кодами без перекрытий [11,12].

Для облегчения чтения статьи мы не только приведем ниже ее краткий план, но и дадим простую комбинаторную постановку исследуемой задачи. Начнем с последнего. Рассмотрим множество (код) C из M "наборов", где каждый набор состоит из n ящиков, занумерованных от 1 до n, в каждом ящике лежит не более одного раскрашенного шара (шары раскрашены в q цветов), а общее число шаров в любом наборе равно w (вес набора). Любое подмножество (коалиция) $U \subset C$ наборов может породить новый набор (набор-потомок) в соответствии со следующими правилами:

1) набор-потомок также состоит из n ящиков, занумерованных от 1 до n;

2) в любой ящик коалиция может положить только один из шаров, имеющихся у нее в ящике с тем же номером, или же не положить ни одного шара (главное правило);

3) общее число шаров в наборе-потомке (т.е. *вес* набора) не меньше w.

Обозначим через $\langle U \rangle$ множество всех наборов-потомков, которые может породить коалиция U в соответствии с правилами 1–3. Будем называть код C t-хорошим (t-IPP), если для любой коалиции мощности не более t и любого ее набора-потомка *все* коалиции мощности не более t из кода C, которые могут породить данный набор-потомок, имеют как минимум один общий для всех набор. Более формально, для любого набора $\boldsymbol{z}$ веса не менее w либо

$$\bigcap_{\substack{U\colon U\subset C,\\ |U|\leqslant t,\ \boldsymbol{z}\in\langle U\rangle}} U \neq \varnothing, \tag{2}$$

либо нет коалиции мощности не более t, для которой набор $\boldsymbol{z}$ является ее потомком.

Основная задача, как обычно, состоит в нахождении кодов максимальной мощности $M_t(n, w; q)$.

Статья организована следующим образом: в § 2 описана математическая постановка задачи, включая определение новой общей ПП-схемы. В § 3 изучается частный случай коалиций из двух участников. В § 4 приводится сравнение с ранее известными ПП-схемами, в § 5 даются заключительные замечания. Описание работы ПП-схем и связь со схемами разделения секрета вынесены в Приложение.

§ 2. IPP-коды, IPP-системы множеств и их обобщение

Напомним определение и основные свойства IPP-кодов, введенных в [2]. Пусть $\mathcal{A}$ – конечный алфавит из q элементов, а $\mathcal{A}^n$ – множество всех слов длины n в алфавите $\mathcal{A}$. Для произвольного множества $U \subset \mathcal{A}^n$ и координаты $j \in \{1, \ldots, n\}$ опре-

делим j-ю проекцию $P_j(U)$ подмножества U как

$$P_j(U) = \bigcup_{\boldsymbol{u} \in U} u_j \tag{3}$$

и определим выпуклую оболочку $\langle U \rangle$ множества U (также называемую узкой оболочкой [13]) как

$$\langle U \rangle = \{\boldsymbol{x} = (x_1, \ldots, x_n) : \, x_j \in P_j(U), \; \forall j\} = P_1(U) \times \ldots \times P_n(U). \tag{4}$$

Пусть $d(x, y)$ – расстояние Хэмминга между векторами $x, y \in \mathcal{A}^n$, определяемое как число позиций, в которых эти векторы не совпадают, т.е. $d(x, y) = |\{i : x_i \neq y_i\}|$. Оболочка (4) называется выпуклой, так как для точек $u, v \in \mathcal{A}^n$ естественно определить соединяющий их "отрезок"

$$[u, v] := \{x \in \mathcal{A}^n : \, d(u, x) + d(x, v) = d(u, v)\},$$

который совпадает с $\langle \{u, v\} \rangle$ (см. [14]). В содержательной постановке задачи множество U – это коалиция недобросовестных пользователей, а $\langle U \rangle$ – множество всех поддельных декодеров (векторов), которое может породить коалиция U, также называемых потомками [2], откуда и терминология "отождествления родителей".

О п р е д е л е н и е 1 [2]. Код $C \subset \mathcal{A}^n$ называется q-ичным кодом, отождествляющим родителей, порядка t (q-ичным t-IPP-кодом), если для любого $\boldsymbol{z} = (z_1, \ldots, z_n) \in \in \mathcal{A}^n$ либо

$$\bigcap_{\substack{U: \, U \subset C, \\ |U| \leqslant t, \, \boldsymbol{z} \in \langle U \rangle}} U \neq \varnothing, \tag{5}$$

либо нет коалиции $U \subset C$, такой что $\boldsymbol{z} \in \langle U \rangle$ и $|U| \leqslant t$.

Следовательно, если дистрибьютор раздаст пользователям в качестве "декодеров" слова t-IPP-кода, то по любому поддельному декодеру $\boldsymbol{z}$, созданному коалицией U, $|U| \leqslant t$, т.е. $\boldsymbol{z} \in \langle U \rangle$, дистрибьютор сможет безошибочно найти как минимум одного пользователя из U.

Хорошо известно, что t-IPP-код при $q \leqslant t$ имеет не более чем q слов. Повторим соответствующее рассуждение, так как оно понадобится нам ниже. Итак, пусть $q \leqslant t$, и пусть C – q-ичный t-IPP-код мощности $|C| \geqslant t + 1$. Рассмотрим произвольную коалицию $U = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_t\} \subset C$ мощности t. Ее члены выбирают в качестве $\boldsymbol{u}_{t+1}$ любой вектор из $C \setminus U$ (код C один, и он всем известен) и порождают вектор $\boldsymbol{z}$, полагая $z_j = \alpha_j$, где α_j – наиболее часто встречающееся значение в j-й координате у векторов $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{t+1}\}$ (будем называть это мажоритарной атакой). Так как $q \leqslant t$, то это значение встречается как минимум два раза, и следовательно, $\boldsymbol{z} \in \langle U^i \rangle$ для всех $i = 1, \ldots, n + 1$, где $\langle U^i \rangle := \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_{t+1}\}$. Но все эти коалиции не пересекаются, т.е. свойство (5) не выполнено, что приводит к противоречию.

Таким образом, не существует нетривиальных двоичных t-IPP-кодов. Это послужило мотивом рассмотрения так называемых *кодов цифровых отпечатков пальцев* (см. [13, 15, 16]). Основное отличие от IPP-кодов заключается в том, что идентификация виновных пользователей допускается с ненулевой вероятностью ошибки (стремящейся к нулю с ростом длины кодов). Для такой модели (которая далее не рассматривается в этой статье) код цифровых отпечатков пальцев – это не один код, а целое семейство кодов, где код выбирается случайно с некоторым заданным распределением вероятностей, которое известно пользователям, но конкретный выбор кода им неизвестен.

С другой стороны, при $q > t$ существуют t-IPP-коды с экспоненциальным числом кодовых слов, т.е. существуют семейства t-IPP-кодов C_i со скоростями $R_i =$

$= n_i^{-1} \log_q |C_i| \geqslant a > 0$, отделенными от нуля [17, 18]. Как обычно, мы хотим построить семейства кодов с данным t-IPP-свойством и максимально возможной скоростью. Нас будет интересовать асимптотика максимальной скорости, когда размер алфавита q фиксирован, а длина кода растет. Обзор результатов, касающихся "обратного" процесса, т.е. когда длина кода фиксирована, а размер алфавита q растет, см. в [19].

В работах [3, 4] на основе общей пороговой (w, n)-схемы разделения секрета была предложена другая ПП-схема, получившая название t-IPP-системы множеств, формальное определение которой дано ниже.

Рассмотрим семейство $\boldsymbol{F} = \{F_1, \ldots, F_M\}$, состоящее из некоторых w-подмножеств множества $\{1, \ldots, n\}$. Для произвольного подмножества ("коалиции") $U \subset \boldsymbol{F}$ множеств из семейства $\boldsymbol{F}$ определим множество $\langle U \rangle_{\text{set}}$ его "потомков" как

$$\langle U \rangle_{\text{set}} = \left\{ B \subset \{1, \ldots, n\} : \; B \subseteq \bigcup_{F \in U} F, \; |B| \geqslant w \right\}. \tag{6}$$

Определение 2 [4]. Семейство $\boldsymbol{F} = \{F_1, \ldots, F_M\}$ w-подмножеств множества $\{1, \ldots, n\}$ называется t-IPP-системой w-множеств, если для любого $D \subset \{1, \ldots, n\}$, такого что $|D| \geqslant w$, либо

$$\bigcap_{U \subset \boldsymbol{F}: \, D \in \langle U \rangle_{\text{set}}, \, |U| \leqslant t} U \neq \varnothing, \tag{7}$$

либо нет $U \subset \boldsymbol{F}$, такого что $|U| \leqslant t$ и $D \in \langle U \rangle_{\text{set}}$.

Другими словами, семейство $\boldsymbol{F}$, состоящее из некоторых w-подмножеств множества $\{1, \ldots, n\}$ является t-IPP-системой w-множеств, если для любого w-подмножества, принадлежащего объединению множеств из некоторой неизвестной t-коалиции из $\boldsymbol{F}$, хотя бы одно из этих множеств (т.е. участник коалиции) может быть однозначно определено. В частности, это означает, что никакой элемент из $\boldsymbol{F}$ не принадлежит объединению t других множеств из $\boldsymbol{F}$. Такие семейства известны как семейства множеств без перекрытий (cover-free sets) [11, 12], а в теории кодирования как дизъюнктивные (или"superimposed") коды [9, 10].

Эквивалентно, вместо семейств множеств можно рассматривать двоичные равновесные коды, сопоставив множествам $F_1, \ldots, F_M$ их характеристические векторы $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_M$. Рассмотрим равновесный код $C = C_{\boldsymbol{F}} = \{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_M\}$ длины n и веса w, состоящий из этих векторов. Будем говорить про двоичные векторы $\boldsymbol{x} = (x_1, \ldots, x_n)$ и $\boldsymbol{y} = (y_1, \ldots, y_n)$, что $\boldsymbol{x}$ больше $\boldsymbol{y}$, и обозначать $\boldsymbol{x} \succ \boldsymbol{y}$, если $x_i \geqslant y_i$ для всех i. Очевидно, что $\boldsymbol{x} \succ \boldsymbol{y}$, если и только если $\boldsymbol{x} \vee \boldsymbol{y} = \boldsymbol{x}$. Для произвольного подмножества (коалиции) $U \subset C$ кода C определим множество потомков $\langle U \rangle_{\text{set}}$ как

$$\langle U \rangle_{\text{set}} = \{\boldsymbol{y} \in \{0,1\}^n : \; \text{wt}(\boldsymbol{y}) \geqslant w, \; \boldsymbol{U} \succ \boldsymbol{y}\}, \tag{8}$$

где $\boldsymbol{U} := \bigvee_{\boldsymbol{u} \in U} \boldsymbol{u}$. Тогда определение 2 можно переписать следующим образом.

Определение 3. Двоичный равновесный код C длины n и веса w называется (t, w)-IPP-кодом, если для любого двоичного вектора $\boldsymbol{z} \in \{0,1\}^n$ веса не менее w либо

$$\bigcap_{U \subset C: \, \boldsymbol{z} \in \langle U \rangle_{\text{set}}, \, |U| \leqslant t} U \neq \varnothing, \tag{9}$$

либо нет $U \subset C$, такого что $|U| \leqslant t$ и $\boldsymbol{z} \in \langle U \rangle_{\text{set}}$.

Замечание 1. Двоичный равновесный (t, w)-IPP-код длины n и q-ичный t-IPP-код несравнимы в следующем смысле: $\langle U\rangle_{\text{set}} \setminus \langle U\rangle \neq \varnothing$ и $\langle U\rangle \setminus \langle U\rangle_{\text{set}} \neq \varnothing$.

Действительно, в модели потомков (8) для двоичных равновесных кодов, т.е. для систем множеств, i-я координата потомка может быть равна нулю, даже если все векторы из коалиции равны 1, что невозможно в модели (4) для IPP-кодов. С другой стороны, в модели (4) для IPP-кодов i-я координата потомка может быть равна нулю, если эта координата хотя бы у одного вектора из коалиции равна нулю, и следовательно, ограничение на вес не обязано выполняться (например, мажоритарная атака может породить нулевой вектор).

Новый более общий класс ПП-схем будет получен ниже как обобщение двоичных равновесных кодов на недвоичный случай при соответствующем определении множества "потомков", которые могут быть порождены коалицией. Нам будет удобно рассматривать $(q+1)$-ичный алфавит как $\mathbb{Z}_{q+1}$, так как символ 0 будет играть специальную роль.

Для произвольного множества $U \subset \mathbb{Z}_{q+1}^n$ пусть, как и прежде, $P_j(U)$ обозначает его j-ю проекцию (см. (3)). Определим для множества U его j-ю *ненулевую* проекцию

$$P_j^{\times}(U) := P_j(U) \setminus \{0\} \tag{10}$$

и *расширенную* проекцию

$$P_j^{*}(U) := P_j(U) \cup \{0\} = P_j^{\times}(U) \cup \{0\}. \tag{11}$$

Будем предполагать, что коалиция U может породить любой вектор из следующего множества

$$\langle U\rangle^{*} := \{y \in P_1^{*}(U) \times \ldots \times P_n^{*}(U) : \operatorname{wt}(y) \geqslant w\}. \tag{12}$$

Сформулируем соответствующее свойство IPP.

Определение 4. Равновесный $(q+1)$-ичный код $C \subset \{0, 1, \ldots, q\}^n$ веса w называется $(t, w)_q$-IPP-кодом, если для любого $\boldsymbol{z} \in \{0, 1, \ldots, q\}^n$, такого что $\operatorname{wt}(\boldsymbol{z}) \geqslant w$, либо

$$\bigcap_{U \subset C:\, \boldsymbol{z} \in \langle U\rangle^{*},\, |U| \leqslant t} U \neq \varnothing, \tag{13}$$

либо нет такого $U \subset C$, что $|U| \leqslant t$ и $\boldsymbol{z} \in \langle U\rangle^{*}$.

Замечание 2. При $q = 1$ это определение совпадает с определением двоичных (t, w)-IPP-кодов или t-IPP-систем w-множеств, а при $w = n$ – с определением q-ичных t-IPP-кодов.

Нам будет удобно обобщить определение $(t, w)_q$-IPP-кода, расширив возможности коалиций. А именно, для произвольного множества $U \subset \mathbb{Z}_{q+1}^n$ определим множество $\langle U\rangle_{w'}^{*}$ его w'-потомков следующим образом:

$$\langle U\rangle_{w'}^{*} := \{y \in P_1^{*}(U) \times \ldots \times P_n^{*}(U) : \operatorname{wt}(y) \geqslant w'\}. \tag{14}$$

Определение 5. Равновесный $(q+1)$-ичный код $C \subset \{0, 1, \ldots, q\}^n$ веса w называется $(t, w, w')_q$-IPP-кодом, если для любого $\boldsymbol{z} \in \{0, 1, \ldots, q\}^n$, такого что $\operatorname{wt}(\boldsymbol{z}) \geqslant w'$, либо

$$\bigcap_{U:\, \boldsymbol{z} \in \langle U\rangle_{w'}^{*},\, |U| \leqslant t,\, U \subset C} U \neq \varnothing, \tag{15}$$

либо нет такого $U \subset C$, что $|U| \leqslant t$ и $\boldsymbol{z} \in \langle U\rangle_{w'}^{*}$.

Замечание 3. Очевидно, что $(t, w, w')_q$-IPP-код при $w \geqslant w'$ является $(t, w)_q$-IPP-кодом.

§ 3. Случай коалиции из двух пользователей

В этом параграфе рассмотрим простейший случай, когда размер коалиции равен всего лишь 2. Даже этот случай не так прост и заслуживает отдельного рассмотрения – см. [2], где впервые были определены и исследованы 2-IPP-коды, и [20], где рассматривались 2-IPP-коды с дополнительным свойством нахождения участника коалиции декодированием по минимуму расстояния (так называемое свойство traceability). Мы выведем асимптотическую нижнюю границу на скорость $(2, w)_q$-IPP-кодов и сравним полученные результаты с ранее известными, а именно с нижними границами для q-ичных 2-IPP-кодов [2] и для 2-IPP-систем w-множеств [21,22].

Под скоростью кода длины n и мощности M будем понимать, как обычно, величину $R = n^{-1} \log_2 M$. Отметим, что мы рассматриваем только *двоичную* скорость, т.е. логарифм берется по основанию 2. Обозначим через $R_t^q(n)$, $R_{t,w}(n)$ и $R_{t,w}^q(n)$ наибольшую возможную скорость q-ичных t-IPP-кодов, t-IPP-систем w-множеств и $(t, w)_q$-IPP-кодов соответственно. Из замечания 1 следует, что $R_{t,n}^q(n) = R_t^q(n)$ и $R_{t,w}^1(n) = R_{t,w}(n)$.

Следующие известные нижние границы являются аналогами границы Варшамова – Гилберта и были получены методом случайного кодирования с выбрасыванием. Для скорости наилучшего q-ичного 2-IPP-кода [2] (случай двух предателей) известно, что

$$R_2^q(n) \geqslant 3^{-1} \log_2 \frac{q^3}{4q^2 - 6q + 3} + o(1), \tag{16}$$

и в частности, $R_2^3(n) \geqslant 3^{-1} \log_2(9/7) + o(1) = 0{,}121 + o(1)$.

Для t-IPP-систем w-множеств естественно максимизировать скорость по параметру w, т.е. рассмотреть величину $\bar{R}_t(n) = \max\limits_w R_{t,w}(n)$. Известно, что $\bar{R}_2(n) \geqslant$ $\geqslant 0{,}036$ и эта скорость достигается при $w/n = 0{,}1156$ [22].

Воспользуемся следующим наблюдением, доказанным в [2] для 2-IPP-кодов, которое также справедливо для рассматриваемых ниже $(2, w)_q$-IPP- и $(2, w, w')_q$-IPP-кодов.

Предложение. *$(q+1)$-ичный код C является $(2, w)_q$-IPP-кодом тогда и только тогда, когда выполнены следующие два свойства*:

1. *Для любых четырех различных упорядоченных кодовых векторов a, b, c, d справедливо*

$$\langle\{a, b\}\rangle^* \cap \langle\{c, d\}\rangle^* = \varnothing; \tag{17}$$

2. *Для любых трех различных упорядоченных кодовых векторов a, b, c справедливо*

$$\langle\{a, b\}\rangle^* \cap \langle\{a, c\}\rangle^* \cap \langle\{b, c\}\rangle^* = \varnothing. \tag{18}$$

Другими словами, у двух пар $\{a, b\}$ и $\{c, d\}$ нет общего "потомка", так же как и у трех пар $\{a, b\}$, $\{b, c\}$ и $\{c, a\}$ тоже нет общего "потомка".

Действительно, для любого вектора z определим граф с множеством вершин, состоящим из слов кода C, в котором вершины $a, b \in C$ соединены ребром, если $z \in \langle\{a, b\}\rangle^*$ (т.е. z является потомком пары $\{a, b\}$). Условие (17) означает, что любые два ребра имеют общую вершину, а условие (18) означает, что в графе нет треугольников. Тогда очевидно, что такой граф – либо звезда, либо пустой граф.

Заметим, что этот же результат справедлив и для $(2, w, w')_q$-IPP-кодов, если в формулах (17) и (18) заменить $\langle\{x, y\}\rangle^*$ на $\langle\{x, y\}\rangle_{w'}^*$. Используя приведенное выше

предложение и метод случайного кодирования, мы докажем следующую асимптотическую нижнюю границу. Пусть, как обычно, $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ – функция двоичной энтропии.

Теорема. *Для любых $q \geqslant 2$ и $\omega \in (0,1]$ найдется n_0, такое что для любого $n \geqslant n_0$ существует $(q+1)$-ичный $(2, (\omega + o(1))n)_q$-IPP-код со скоростью $R(\omega) = \min\{R_3, R_4\} + o(1)$, где*

$$R_3 = -\frac{1}{2}\left(H(\omega) + \omega\log_2 p + (1-\omega)\log_2(1-p)\right),$$

$$R_4 = -\frac{1}{3}\left(H(\omega) + \omega\log_2 \mathcal{P} + (1-\omega)\log_2(1-\mathcal{P})\right),$$

$$p = \frac{\omega^2}{q^2}(3q-2\omega), \quad \mathcal{P} = \frac{4}{q}\omega^2 - \frac{4}{q^2}\omega^3 - \frac{2q-3}{q^3}\omega^4.$$

Доказательство. Рассмотрим случайный $(q+1)$-ичный код мощности M, в котором координаты кодовых слов порождены независимо с одинаковым распределением вероятностей, при этом вероятность появления символа 0 равна ρ, и каждый ненулевой символ появляется с вероятностью ω/q, где $\rho + \omega = 1$. Опираясь на предложение, мы будем доказывать существование $(2, w, w')_q$-IPP-кодов, где $w' \leqslant w$, с помощью метода случайного кодирования с выбрасыванием (см. [23]) таким образом, чтобы получить код со следующими тремя свойствами: во-первых, в нем все четверки векторов хорошие, т.е. выполнено (17); во-вторых, в нем все тройки векторов хорошие, т.е. выполнено (18); в-третьих, код является равновесным веса $w' = \omega' n \leqslant w$, где параметр $\omega' = \omega + o(1)$ будет выбран в конце доказательства.

Начнем с анализа условия (17). Будем говорить, что четверка различных векторов $\{a, b, c, d\}$ *плохая*, если пары $\{a, b\}$ и $\{c, d\}$ могут породить один и тот же вектор z веса w' (или больше). Будем говорить, что i-я координата *плохая* для данной четверки различных векторов $\{a, b, c, d\}$, если

$$P_i^{\times}(\{a_i, b_i\}) \cap P_i^{\times}(\{c_i, d_i\}) \neq \varnothing, \tag{19}$$

т.е. в этой координате пары имеют хотя бы одно одинаковое ненулевое значение, которое и может быть использовано для порождения общего вектора-потомка z. Таким образом, условие "упорядоченная четверка различных векторов плохая" равносильно тому, что число плохих координат у этой четверки не меньше w'.

Оценим вероятность p_{good} того, что i-я координата является "хорошей", т.е. эти две пары не имеют одинаковых ненулевых значений в i-й координате. Это возможно в следующих четырех ситуациях:

1. $a_i = b_i = 0$, а значения c_i, d_i могут быть любыми, и наоборот. Вероятность такого события равняется $p_1 = 2\rho^2 - \rho^4$ (так как случай $a_i = b_i = c_i = d_i = 0$ считается дважды);
2. Каждая пара имеет одно нулевое и одно ненулевое значение в i-й координате, причем эти ненулевые значения различны. Например, $a_i = 0$, $b_i = 1$ и $c_i = 0$, $d_i = 2$. Вероятность такого события равняется $p_2 = 4(\rho\omega)^2(1 - 1/q)$;
3. Одна пара имеет одно нулевое и одно ненулевое значение в i-й координате, другая пара имеет два ненулевых значения, отличных от первой пары, например, $a_i = 0$, $b_i = 1$ и $c_i = 2$, $d_i = 3$. Вероятность такого события равняется $p_3 = 4\rho\omega^3(1-1/q)^2$;
4. Обе пары имеют только ненулевые значения, причем множества $\{a_i, b_i\}$ и $\{c_i, d_i\}$ "разделены", т.е. $\{a_i, b_i\} \cap \{c_i, d_i\} = \varnothing$, например, $a_i = 1$, $b_i = 2$ и $c_i = 3$, $d_i = 3$. Вероятность такого события равняется

$$p_4 = \omega^4\left((1-1/q)(1-2/q)(1-3/q) + \frac{2}{q}(1-1/q)(1-2/q) + \frac{1}{q^2}(1-1/q)\right) =$$
$$= \omega^4(q^3 - 4q^2 + 6q - 3)/q^3.$$

Таким образом, вероятность того, что i-я координата хорошая, равна

$$p_{\text{good}} = \sum_{i=1}^{4} p_i = 2\rho^2 - \rho^4 + 4(\rho\omega)^2(1-1/q) + 4\rho\omega^3(1-1/q)^2 +$$
$$+ \frac{\omega^4}{q^3}(q^3 - 4q^2 + 6q - 3) = 1 + \frac{2q-3}{q^3}\omega^4 + \frac{4}{q^2}\omega^3 - \frac{4}{q}\omega^2,$$

а вероятность того, что координата плохая, –

$$\mathcal{P} = 1 - p_{\text{good}} = \frac{4}{q}\omega^2 - \frac{4}{q^2}\omega^3 - \frac{2q-3}{q^3}\omega^4. \tag{20}$$

Так как четверка векторов плохая, если для нее найдется по крайней мере $w' = \omega' n$ плохих координат, то соответствующая вероятность $\mathcal{P}_4$ имеет вид

$$\mathcal{P}_4 = \sum_{j \geqslant \omega' n} \binom{n}{j} \mathcal{P}^j (1-\mathcal{P})^{n-j}. \tag{21}$$

Чтобы оценить $\mathcal{P}_4$ сверху, воспользуемся известным неравенством

$$\sum_{j \geqslant \sigma n} \binom{n}{j} \mathcal{P}^j (1-\mathcal{P})^{n-j} \leqslant 2^{-nD(\sigma||\mathcal{P})}, \tag{22}$$

справедливым при $\sigma > \mathcal{P}$, где $D(\sigma||\mathcal{P}) = \sigma\log_2(\sigma/\mathcal{P}) + (1-\sigma)\log_2((1-\sigma)/(1-\mathcal{P}))$ – дивергенция Кульбака – Лейблера. Заметим, что $\mathcal{P} < \omega$ для любых $q \geqslant 2$ и $\omega \in (0, 1]$. Действительно,

$$\mathcal{P} - \omega = \omega\left(-1 + \frac{4\omega}{q} - \frac{4\omega^2}{q^2} - (2q-3)(\omega/q)^3\right) < -w\left(1 - \frac{2\omega}{q}\right)^2 \leqslant 0, \tag{23}$$

где строгое неравенство возникает из-за того, что $(2q-3)(\omega/q)^3 > 0$ при $q \geqslant 2$. Так как ω' будет ниже выбрано так, чтобы $\omega' = \omega + o(1)$, то $\omega' > \mathcal{P}$ для достаточно больших n, и применение неравенства (22) дает следующую верхнюю оценку:

$$\mathcal{P}_4 \leqslant 2^{nH(\frac{w'}{n})} \mathcal{P}^{w'} (1-\mathcal{P})^{n-w'}. \tag{24}$$

Следовательно, для математического ожидания числа плохих четверок $E_4 = E_4(M)$ справедливо неравенство

$$E_4 := \mathbf{E}(\#\text{ плохих четверок}) \leqslant M^4 2^{nH(\frac{w'}{n})} \mathcal{P}^{w'} (1-\mathcal{P})^{n-w'}. \tag{25}$$

Пусть M_4 обозначает максимальное целое число M, такое что $E_4(M) \leqslant M/(4n)$. Неравенство (25) дает следующую оценку на M_4:

$$M_4^3 2^{nH(\frac{w'}{n})} \mathcal{P}^{w'} (1-\mathcal{P})^{n-w'} \geqslant \frac{1}{4n},$$

и при $n \to \infty$ получаем, что

$$n^{-1}\log M_4 \geqslant R_4 := -\frac{1}{3}\big(H(\omega') + \omega'\log_2\mathcal{P} + (1-\omega')\log_2(1-\mathcal{P})\big).$$

Пусть $M \leqslant M_4$. Удалим из каждой плохой четверки один вектор. Тогда оставшаяся часть кода не будет содержать плохих четверок, и согласно неравенству Маркова вероятность того, что результирующий код (без плохих четверок) будет иметь мощность менее $\frac{3}{4}M$, не превосходит $1/n$.

Теперь рассмотрим условие (18). А именно, рассмотрим три различных вектора a, b, c, таких что все три пары $\{a, b\}$, $\{b, c\}$ и $\{a, c\}$ могут породить один и тот же вектор z веса по крайней мере w'. Вычислим вероятность того, что i-я координата является плохой, т.е. вероятность события

$$P_i^{\times}(\{a_i, b_i\}) \cap P_i^{\times}(\{b_i, c_i\}) \cap P_i^{\times}(\{c_i, a_i\}) \neq \varnothing. \tag{26}$$

Ясно, что если из трех значений a_i, b_i, c_i хотя бы два нулевые, то эта координата всегда хорошая. Если одно из трех значений координаты нулевое, то эта координата плохая в том случае, когда два ненулевых значения одинаковы, например, $a_i = 0$, $b_i = 1$, $c_i = 1$. Эта вероятность равна $3\rho\omega^2/q$. Наконец, если все три значения данной координаты ненулевые, то эта координата хорошая в том случае, когда эти три значения различны. Вероятность этого события равна $\omega^3(1 - 1/q)(1 - 2/q)$. Следовательно, вероятность того, что все три координаты ненулевые и эта координата плохая, равна $\omega^3(3/q - 2/q^2)$.

Итак, вероятность p того, что данная координата плохая, равна

$$p = 3\rho\omega^2/q + \omega^3(3/q - 2/q^2) = \frac{\omega^2}{q}\left(3 - \frac{2\omega}{q}\right). \tag{27}$$

Так как упорядоченная тройка векторов плохая, если для нее найдется по крайней мере $w' = \omega' n$ плохих координат, то соответствующая вероятность $\mathcal{P}_3$ равна

$$\mathcal{P}_3 = \sum_{j \geqslant \omega' n} \binom{n}{j} p^j (1 - p)^{n-j}. \tag{28}$$

Аналогично предыдущему случаю нетрудно убедиться, что для любого $q \geqslant 2$ и $\omega \in (0, 1]$ верно, что $p < \omega$. Применение неравенства (22) приводит к следующей верхней оценке:

$$\mathcal{P}_3 \leqslant 2^{nH(\frac{w'}{n})} p^{w'} (1 - p)^{n-w'}, \tag{29}$$

и среднее число плохих троек можно оценить сверху как

$$E_3 = E_3(M) := \mathbf{E}(\#\text{ плохих троек}) \leqslant M^3 2^{nH(\frac{w'}{n})} p^{w'} (1 - p)^{n-w'}. \tag{30}$$

Пусть M_3 обозначает максимальное M, такое что $E_3 \leqslant M/(8n)$. Неравенство (30) дает следующую оценку на M_3:

$$M_3^2 2^{H(\frac{w'}{n})} p^{w'} (1 - p)^{n-w'} \geqslant \frac{1}{8n},$$

и при $n \to \infty$ получаем, что

$$R_3 := n^{-1} \log M_3 = -\frac{1}{2}\big(H(\omega') + (1 - \omega') \log_2(1 - p) + \omega' \log_2(p)\big).$$

Пусть $M \leqslant M_3$. Удалим из каждой плохой тройки один вектор. Тогда оставшаяся часть кода не будет содержать плохих троек векторов, и согласно неравенству Маркова вероятность того, что результирующий код (без плохих троек) имеет мощность менее $\frac{7}{8}M$, не превосходит $1/n$.

Третий этап "выбрасывания" состоит в исключении кодовых слов нетипичного веса. А именно, оставим в коде только слова веса не менее $w' := \omega n - \sqrt{n \ln n}$ и не более $w'' := \omega n + \sqrt{n \ln n}$. Согласно неравенству Хеффдинга [24] вероятность того, что случайный вектор имеет вес в диапазоне $[w', w'']$, не меньше $1 - \frac{2}{n^2}$. Применив

неравенство Маркова, получим, что число нетипичных векторов будет не больше $\frac{1}{8}M$ с вероятностью не меньше $1-\frac{16}{n^2}$.

Следовательно, если положить $M=\min\{M_3,M_4\}$ и применить все три исключения, то результирующий код будет иметь мощность не менее $M/2$ с вероятностью $1-\frac{3}{n}$ при $n\geqslant 16$.

Заметим, что полученный код не обязан быть равновесным. Поэтому разделим код на подкоды, состоящие из слов одинакового веса, и выберем среди них подкод максимальной мощности. Этот код будет равновесным кодом с весом $w^*\in[w',w'']$ мощности не менее $(4\sqrt{n\ln n})^{-1}M$, т.е. будет иметь ту же асимптотическую скорость и все желаемые свойства, что и завершает доказательство. ▲

Рассмотрим отдельно случай $q=1$, т.е. случай 2-IPP-систем множеств. Все рассуждения теоремы справедливы вплоть до неравенства (23), которое при $q=1$ примет вид

$$\mathcal{P}-\omega=\omega(-1+4\omega-4\omega^2+\omega^3)=\omega(\omega-1)(\omega^2-3\omega+1), \tag{31}$$

и в диапазоне $\omega\in(0,1]$ мы имеем, что $\mathcal{P}-\omega<0$ только при $\omega\in\Big(0,\frac{3-\sqrt{5}}{2}\Big]$. Итоговая оценка на скорость $R(\omega)=\min\{R_3,R_4\}+o(1)$, задаваемая теоремой, остается справедливой, и максимум скорости достигается при $\omega=0{,}062$ и равен $0{,}0211$.

§ 4. Как сравнить различные схемы поиска предателей?

Чтобы сравнить различные ПП-схемы, описанные в данной статье, вернемся к работе [1], где было предложено рассматривать общее число переданных зашифрованных долей как "длину блока" N и соответственно определить *эффективную* скорость как

$$R_{\mathrm{ef}}=N^{-1}\log_2 M, \tag{32}$$

где M обозначает мощность соответствующего кода. Для $(t,w)_q$-IPP-кодов и q-ичных IPP-кодов $N=nq$, а для IPP-систем множеств $N=n$. Это означает, что для q-ичных IPP-кодов и для новой ПП-схемы, чтобы получить их эффективную скорость, нужно поделить их обычную (двоичную) скорость на q, а в случае IPP-систем множеств обычная и эффективная скорости совпадают.

Рассмотрим более подробно случай $t=2$. Анализ поведения функций R_3 и R_4 при $q=2$ показывает, что минимум двух скоростей достигается на R_4 до точки пересечения ($\omega=0{,}861$), а затем на R_3. При $\omega\to 1$ получаем, что скорость $R\to 0$, что, как мы уже отмечали выше, означает, что хороших двоичных IPP-кодов ($\omega=1$ и $q=2$) не существует. Максимум $R_{\mathrm{ef}}(\omega)$ по $\omega\in[0,1]$ достигается в точке $\omega=0{,}135$ и равен $0{,}0218$.

При $q=3$ скорость $R(\omega)=\min\{R_3,R_4\}=R_4$ при всех ω, достигает своего максимума при $\omega=1$, т.е. на троичных 2-IPP-кодах, и равна $R(1)=0{,}1206$, что, конечно, совпадает с известной нижней оценкой для троичных 2-IPP-кодов [2]. Следовательно, эффективная скорость $R_{\mathrm{ef}}\geqslant 0{,}0402$.

При фиксированном $q>3$ максимальное значение R, задаваемое теоремой, также всегда достигается при $\omega=1$, т.е. на q-ичных IPP-кодах. При этом максимальная эффективная скорость достигает своего максимума при $q=7$ и равняется $R_{\mathrm{ef}}=$ $=0{,}0536$.

Отметим, что при любом фиксированном t эффективная скорость стремится к 0 при растущем основании кода q, так как

$$R_{\mathrm{ef}} = \frac{\log_2 M}{nq} = \frac{\log_q M}{n}\,\frac{\log_2 q}{q} \leqslant \frac{\log_2 q}{q}. \tag{33}$$

§ 5. Заключение

В статье предложена новая общая схема поиска предателей с нулевой вероятностью ошибки. Она обобщает две ранее известные ПП-схемы: q-ичные t-IPP-коды и t-IPP-системы множеств, и ее можно рассматривать как равновесные q-ичные t-IPP-коды или как q-"раскрашенные" t-IPP-системы w-множеств.

Случай $t = 2$ (двух предателей) и произвольного q являлся предметом отдельного исследования в данной статье. Оказалось, что если сравнивать скорости, получаемые из соответствующих аналогов границы Варшамова – Гилберта, то наилучший результат дают 7-ичные 2-IPP-коды.

Неизвестно, существует ли пример наилучшей ПП-схемы с $1 < w < n$, или же экстремум всегда достигается в крайних точках $w = 1$ или $w = n$, т.е. на q-ичных t-IPP-кодах или на t-IPP-системах множеств.

Обобщение теоремы на случай произвольного t является предметом дальнейшего исследования. В случае обычных IPP-кодов это было сделано в работе [13] с помощью специально введенного понятия частичных хэш-функций.

ПРИЛОЖЕНИЕ

Пороговые схемы разделения секрета как основа IPP-схем поиска предателей. Вернемся к модели широковещательной передачи цифрового контента, кратко описанной в § 1. Чтобы предотвратить незаконную перепродажу и распространение контента x, дистрибьютор передает x в зашифрованном виде как $y = \varphi(x, k)$, полученном с помощью отображения шифрования $\varphi(\cdot\,, k)$ и некоторого *секрета* $k \in \mathcal{K}$, который нужно изменять для передачи других частей цифрового контента. В действительности дистрибьютор заменяет задачу защищенной широковещательной передачи большого файла x на задачу защищенной широковещательной передачи сравнительно маленького файла k. Чтобы распределить секрет k среди пользователей, дистрибьютор сначала "разделяет" его на доли $k_1, \ldots, k_n$ в соответствии с выбранной схемой разделения секрета. Доли шифруются с помощью отображения ψ и соответствующего набора ключей $\mathcal{F} = \{f_1, \ldots, f_N\}$, где j-я доля k_j шифруется с помощью множества ключей $F^{(j)} \subset \mathcal{F}$. Затем полученные зашифрованные доли передаются как некоторые блоки информации $e_1, \ldots, e_N$ вместе с цифровым контентом y. Во время фазы инициализации ℓ-й пользователь получает декодер, состоящий из соответствующего набора ключей F_ℓ, который позволяет дешифровать необходимое число долей k_j, а зная их, найти секрет k, и следовательно, дешифровать x. Ниже мы уточним эту концепцию для рассмотренных в статье схем поиска предателей.

Начнем с t-IPP-кодов. Секрет $k \in \mathcal{K}$ делится на n долей $k_1, \ldots, k_n$ в соответствии с (1). Дистрибьютор зашифровывает каждую долю k_j на q различных ключах, которые образуют множество $F^{(j)} = \{f_{j,1}, \ldots, f_{j,q}\} \subset \mathcal{F}$. Результатом шифрования является последовательность $(e_{j,1}, \ldots, e_{j,q})$, где $e_{j,i} = \psi(k_j, f_{j,i})$ – это i-я зашифрованная версия доли k_j. Всего получаем $N = nq$ зашифрованных долей $\{e_{11}, \ldots, e_{1q}, \ldots, e_{n1}, \ldots, e_{nq}\}$, передаваемых дистибьютором вместе с y. На этапе инициализации ℓ-й пользователь получает определенную последовательность ключей (декодер) $F_\ell = (f_{1,\ell_1}, \ldots, f_{n,\ell_n})$, т.е. каждый пользователь получает ровно по одному ключу из каждого множества ключей $F^{(j)}$ для дешифрования j-й доли. Поэто-

му любой пользователь может восстановить (расшифровать) все доли $\{k_1, \ldots, k_n\}$, затем найти секрет k, а следовательно, и контент x.

Если коалиция предателей $U \subset \{1, \ldots, M\}$ хочет создать декодер, который сможет расшифровывать каждый переданный цифровой контент, то коалиция должна создать новый набор ключей $\boldsymbol{z} = (z_1, \ldots, z_n)$ со свойством $z_j \in F^{(j)}$ для всех $j \in \{1, 2, \ldots, n\}$ и $z_j \in \{f_{ju_j} : u \in U\}$, где последнее означает, что коалиция может выбирать ключи только из имеющегося у нее множества ключей. Первое свойство есть следствие совершенности используемой схемы разделения секрета, т.е. при "нехватке" хотя бы одной доли коалиция не имеет никакой апостериорной информации о секрете k. Второе свойство отражает предположение, что множество всех потенциальных ключей шифрования очень большое, и только дистрибьютору известно, каким участникам какие наборы ключей были выданы. Это соответствует так называемой "узкой оболочке" в терминологии [13].

Для того чтобы переформулировать задачу на языке теории кодирования, занумеруем множество ключей j-й доли $F^{(j)}$ элементами q-ичного алфавита, сопоставим ℓ-му пользователю соответствующий q-ичный вектор номеров его ключей $\boldsymbol{c}_\ell = (\ell_1, \ldots, \ell_n)$, а множество всех векторов, соответствующих пользователям, будем рассматривать как q-ичный код. Тогда описанная выше коалиционная атака на языке векторов означает, что коалиция $U \subset C$ может породить любой вектор $\boldsymbol{z} \in \langle U \rangle$ и только их (см. (4)), что и дает естественное обоснование определению t-IPP-кодов (определение 1).

В основе t-IPP-систем множеств лежит совершенная идеальная пороговая (w, n)-схема [5,6], которая "делит" секрет $k \in \mathcal{K}$ на n "долей" $k_1, \ldots, k_n \in \mathcal{K}$ таким образом, что любые w долей позволяют однозначно найти секрет k, в то время как меньшее число долей не дает никакой апостериорной информации о k. Для того чтобы секретным образом распространить доли среди пользователей, дистрибьютор шифрует каждую долю k_j своим ключом f_j. На этапе инициализации ℓ-й пользователь получает набор $F_\ell = \{f_{\ell_1}, \ldots, f_{\ell_w}\}$ из w ключей, который позволяет дешифровать доли с номерами из множества $X_\ell = \{\ell_1, \ldots, \ell_w\}$, затем найти с их помощью секрет k, и следовательно, восстановить передаваемый цифровой контент x. Сопоставим ℓ-му пользователю множество $X_\ell : |X_\ell| = w$. Любая коалиция U "предателей" для создания поддельного декодера, также способного восстановить любой передаваемый цифровой контент, должна выбрать как минимум w разных ключей из объединения ключей, принадлежащих участникам U. Таким образом, коалиция U должна создать любое множество (ключей) $B \subset \{1, \ldots, n\}$ мощности не менее w, но при этом может создавать только множества $B \subseteq \bigcup\limits_{u \in U} X_u$. Тем самым, коалиционная атака описывается множеством $\langle U \rangle_{\text{set}}$ "потомков" коалиции U (см. (6)), что также дает обоснование определению t-IPP-системам множеств (определение 2).

Заметим, что в модели IPP-систем множеств каждая доля, полученная из секрета k с помощью пороговой (w, n)-схемы разделения секрета, зашифрована с использованием только одного ключа E_j, $j = 1, \ldots, n$, а в модели IPP-кодов каждая доля шифруется с использованием q различных ключей $F^{(j)} = \{f_{j1}, \ldots, f_{jq}\}$. Для создания q-ичных IPP-систем множеств предлагается объединить эти две идеи, а именно:

1. Для восстановления ключа пользователю необходимо иметь как минимум w (из n) долей секрета k;
2. Каждая доля зашифрована с использованием q ключей.

Мы предлагаем реализовать это следующим образом: дистрибьютор делит секрет k на n "долей" $k_1, \ldots, k_n$ с помощью совершенной идеальной пороговой (w, n)-схемы, как и выше при построении t-IPP-систем множеств, но при этом доля k_j шифруется с использованием q различных ключей $F^{(j)} = \{f_{j,1}, \ldots, f_{j,q}\}$, как при построении t-IPP-кодов. В результате шифрования доли k_j дистрибьютор получит после-

довательность $(e_{j,1},\dots,e_{j,q})$, где $e_{j,i}=\psi(k_j,f_{j,i})$ – i-я зашифрованная версия доли k_j. В итоге дистрибьютор передаст вместе с y все $N=nq$ зашифрованных долей $\{e_{1,1},\dots,e_{1,q},\dots,e_{n,1},\dots,e_{n,q}\}$. На этапе инициализации ℓ-й пользователь получает персональную последовательность ключей (декодер) $F_\ell=(f_{j_1,\ell_1},\dots,f_{j_w,\ell_w})$, т.е. каждый пользователь получает ровно по одному ключу из множества ключей $F^{(j)}$, $j\in J_\ell$, для дешифрования j-й доли, и так для всех w долей. Поэтому любой пользователь может восстановить (расшифровать) w долей, затем найти с их помощью секрет k, а следовательно, и контент x.

Занумеруем множество ключей j-й доли $F^{(j)}$ элементами алфавита $\{1,\dots,q\}$, добавив к алфавиту символ 0 и превратив его в $\mathbb{Z}_{q+1}$, и сопоставим ℓ-му пользователю соответствующий $(q+1)$-ичный вектор $\boldsymbol{c}_\ell=(c_1,\dots,c_n)$, где $c_j=\ell_j\in\{1,\dots,q\}$, если ℓ-й пользователь получает ключ f_{j,ℓ_j} для дешифрования j-й доли, и $c_j=0$ в противном случае. Обозначим через C код, состоящий из всех векторов, соответствующих пользователям.

Произвольная коалиция предателей $U\subset C$, чтобы создать декодер, способный расшифровывать любой переданный цифровой контент, должна породить новый набор из не менее чем w ключей, которому соответствует вектор $\boldsymbol{z}=(z_1,\dots,z_n)$ веса не менее w, такой что $z_j\in\Big\{\bigcup\limits_{u\in U}u_j\Big\}=P_j^{\times}(U)$ для $j:z_j\neq 0$ (см. (10)), где последнее свойство означает, как и раньше, что коалиция может порождать ключи только из имеющегося у нее множества ключей. Данная коалиционная атака совпадает с определением (12), а также с правилами 1–3 порождения наборов-потомков (см. § 1), что и приводит к данному в статье общему определению равновесных $(q+1)$-ичных t-IPP-кодов (определение 4).

СПИСОК ЛИТЕРАТУРЫ

1. *Chor B., Fiat A., Naor M.* Tracing Traitors // Advances in Cryptology—CRYPTO'94 (Proc. 14th Annual Int. Cryptology Conf. Santa Barbara, CA, USA. August 21–25, 1994). Lect. Notes Comp. Sci. V. 839. Berlin: Springer, 1994. P. 257–270.
2. *Hollmann H.D.L., van Lint J.H., Linnartz J.-P., Tolhuizen L.M.G.M.* On Codes with the Identifiable Parent Property // J. Combin. Theory Ser. A. 1998. V. 82. № 2. P. 121–133.
3. *Stinson D.R., Wei R.* Combinatorial Properties and Constructions of Traceability Schemes and Frameproof Codes // SIAM J. Discrete Math. 1998. V. 11. № 1. P. 41–53.
4. *Collins M.J.* Upper Bounds for Parent-Identifying Set Systems // Des. Codes Cryptogr. 2009. V. 51. № 2. P. 167–173.
5. *Blakley G.R.* Safeguarding Cryptographic Keys // Proc. 1979 National Computer Conf.: Int. Workshop on Managing Requirements Knowledge. New York. June 4–7, 1979. AFIPS Conf. Proceedings, V. 48. Montvale, NJ: AFIPS Press, 1979. P. 313–317.
6. *Shamir A.* How to Share a Secret // Comm. ACM. 1979. V. 22. № 11. P. 612–613.
7. *Кабатянский Г.А.* Математика разделения секрета // Матем. просв. Сер. 3. 1998. Вып. 2. С. 115–126.
8. *Блейкли Р.Г., Кабатянский Г.А.* Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Пробл. передачи информ. 1997. Т. 33. № 3. Р. 102–110.
9. *Kautz W.H., Singleton R.C.* Nonrandom Binary Superimposed Codes // IEEE Trans. Inform. Theory. 1964. V. 10. № 4. P. 363–377.
10. *Дьячков А.Г., Рыков В.В.* Границы длины дизъюнктивных кодов // Пробл. передачи информ. 1982. Т. 18. № 3. С. 7–13.
11. *Erdős P., Frankl P., Füredi Z.* Families of Finite Sets in Which No Set Is Covered by the Union of Two Others // J. Combin. Theory Ser. A. 1982. V. 33. № 2. P. 158–166.
12. *Erdős P., Frankl P., Füredi Z.* Families of Finite Sets in Which No Set Is Covered by the Union of r Others // Israel J. Math. 1985. V. 51. № 1–2. P. 79–89.

13. *Barg A., Blakley G.R., Kabatiansky G.A.* Digital Fingerprinting Codes: Problem Statements, Constructions, Identification of Traitors // IEEE Trans. Inform. Theory. 2003. V. 49. № 4. P. 852–865.
14. *Körner J.* On the Extremal Combinatorics of the Hamming Space // J. Combin. Theory Ser. A. 1995. V. 71. № 1. P. 112–126.
15. *Boneh D., Shaw J.* Collusion-Secure Fingerprinting for Digital Data // IEEE Trans. Inform. Theory. 1998. V. 44. № 5. P. 1897–1905.
16. *Tardos G.* Optimal Probabilistic Fingerprint Codes // Proc. 35th Annual ACM Sympos. on Theory of Computing (STOC'03). San Diego, CA, USA. June 9–11, 2003. P. 116–125.
17. *Barg A., Cohen G., Encheva S., Kabatiansky G., Zémor G.* A Hypergraph Approach to the Identifying Parent Property: The Case of Multiple Parents // SIAM J. Discrete Math. 2001. V. 14. № 3. P. 423–431.
18. *Alon N., Cohen G., Krivelevich M., Litsyn S.* Generalized Hashing and Parent-Identifying Codes // J. Combin. Theory Ser. A. 2003. V. 104. № 1. P. 207–215.
19. *Blackburn S.R.* Combinatorial Schemes for Protecting Digital Content // Surveys in Combinatorics, 2003 (Proc. 19th British Combinatorial Conf. Univ. of Wales, Bangor, UK. June 29 – July 4, 2003). Lond. Math. Soc. Lect. Note Ser. V. 307. Cambridge, UK: Cambridge Univ. Press, 2003. P. 43–78.
20. *Кабатянский Г.А.* Коды для защиты авторских прав: случай двух пиратов // Пробл. передачи информ. 2005. Т. 41. № 2. С. 123–127.
21. *Gu Y., Miao Y.* Bounds on Traceability Schemes // IEEE Trans. Inform. Theory. 2018. V. 64. № 5. P. 3450–3460.
22. *Egorova E., Kabatiansky G.* Analysis of Two Tracing Traitor Schemes via Coding Theory // Coding Theory and Applications (Proc. 5th Int. Castle Meeting, ICMCTA 2017. Vihula, Estonia. August 28–31, 2017). Lect. Notes Comp. Sci. V. 10495. Cham: Springer, 2017. P. 84–92.
23. *Бассалыго Л.А., Гельфанд С.И., Пинскер М.С.* Простые методы получения нижних границ в теории кодов // Пробл. передачи информ. 1991. Т. 27. № 4. С. 3–8.
24. *Hoeffding W.* Probability Inequalities for Sums of Bounded Random Variables // J. Amer. Statist. Assoc. 1963. V. 58. № 301. P. 13–30.

Егорова Елена Евгеньевна
Сколковский институт науки и технологий
egorovahelene@gmail.com

Поступила в редакцию
06.05.2019
После доработки
23.06.2019
Принята к публикации
25.06.2019