ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 55 **2019** **Вып. 3**

УДК 621.391.15

© 2019 г. **Г.А. Кабатянский**

ИДЕНТИФИЦИРУЮЩИЕ КОДЫ И ИХ ОБОБЩЕНИЯ

Коды с идентификацией "родителей" возникли как одно из решений задачи широковещательного шифрования. Предлагается новая, наиболее общая модель таких кодов, дается обзор известных результатов и формулируются некоторые нерешенные задачи.

Ключевые слова: широковещательное шифрование, схемы разделения секрета, IPP-схемы, разделяющие коды.

DOI: 10.1134/S0555292319030070

§ 1. Введение

Рассмотрим следующую постановку задачи – дистрибьютор D использует широковещательный канал для распространения потока файлов для M авторизованных пользователей. Каждый из авторизованных пользователей имеет персональное устройство – декодер, который позволяет читать (воспроизводить) передаваемые дистрибьютором файлы. Одной из возможных атак со стороны недобросовестных пользователей на такую систему является коалиционная атака, когда группа недобросовестных пользователей (далее – коалиция) создает поддельный декодер для дальнейшего нелегального распространения файлов. Задача коалиции состоит в том, чтобы создать такой поддельный декодер, чтобы *все члены коалиции остались неизвестными*, даже если D получит в свое распоряжение такую подделку. Дистрибьютор же, в свою очередь, хочет создать такое множество декодеров, раздаваемых авторизованным пользователям, чтобы в случае коалиционной атаки он мог по поддельному декодеру безошибочно найти по крайней мере одного участника коалиции. Имеется следующее примитивное и в то же время оптимальное решение этой задачи, если нет никаких ограничений на коалиции, например, на их размер.

Дистрибьютор D передает все файлы в зашифрованном виде, т.е. вместо файла x передается файл $y = F(x, s_0)$, полученный с помощью отображения шифрования $F(\cdot\,,\cdot)$ и некоторого секретного ключа $s_0 \in \mathcal{S}_0$. Ключ s_0, вообще говоря, изменяется для передачи другого файла. Кроме этого, D создает M *различных* зашифрованных копий $g_1, \ldots, g_M$ ключа s_0 с помощью другого отображения шифрования $G(\cdot\,,\cdot)$, где $g_i = G(s_0, k_i)$, а k_i – персональный ключ i-го пользователя, который он получает от D перед началом передачи файлов. Эти M зашифрованных копий присоединяются к файлу y, т.е. в итоге передается следующая последовательность: $y, g_1, \ldots, g_M$. Получив такую последовательность, i-й пользователь дешифрует g_i с помощью своего персонального ключа k_i, тем самым, находит секретный ключ s, а с его помощью дешифрует Y и получает искомый файл X. *Любая* коалиция, чтобы создать декодер, способный читать/воспроизводить передаваемые дистрибьютором файлы, должна предоставить в распоряжение этого декодера хотя бы один из персональных ключей членов коалиции, и следовательно, D способен найти как минимум одного члена

коалиции. Очевидный недостаток такого решения – это большая избыточность, так как D должен передать кроме y (шифрование, как правило, не увеличивает объем файла) еще и M зашифрованных копий $g_1, \ldots, g_M$ ключа s_0.

В работе [1] было предложено решение, позволяющее ограничиться избыточностью порядка $c_t \log M$ при условии, что размер коалиции не превышает t. В основе этого решения лежат совершенные схемы разделения секрета [2, 3] и специальные коды, получившие название *коды со свойством идентификации родителей* (codes with the identifiable parent property) [4], далее для краткости – IPP-коды. Именно IPP-коды в различных вариациях постановки задачи и являются главным объектом данной статьи.

Напомним, что схема разделения секрета "распределяет" в множестве участников $\mathcal{X} = \{1, 2, \ldots, n\}$ некоторый секрет s_0 из множества всех секретов S_0, посылая i-му участнику его "долю" $s_i \in S_i$. При этом участники не знают значения других "долей" секрета. Схема должна позволять разрешенным группам участников восстанавливать секрет, тогда как неразрешенные группы не должны получать из знания их долей секрета никакой апостериорной информации о его значении – такая схема называется *совершенной*, или сокращенно ССРС. Разрешенные группы образуют *монотонную структуру доступа* $\Gamma \subset 2^{\mathcal{X}}$, т.е. из $A \in \Gamma$ и $A \subset B$ следует, что и $B \in \Gamma$. В [2, 3] были построены совершенные схемы для пороговых (w, n)-структур доступа

$$\Gamma_w = \{A \subset \mathcal{X} : \ |A| \geqslant w\}.$$

Эти схемы, в дополнение к совершенности, также являются *идеальными*, т.е. все множества S_i одинаковы и равны S_0.

В [1] для простейшего примера совершенной идеальной пороговой (n, n)-схемы было предложено решение, позднее получившее название IPP-коды [4], позволившее свести задачу широковещательной передачи зашифрованного файла $y = F(x, s_0)$ к задаче широковещательной передачи секрета $s_0 \in S_0$ путем передачи его зашифрованных долей. Позднее этот же подход был применен к общим пороговым ССРС, а соответствующие схемы получили название IPP-системы множеств [5, 6]. Дальнейшее обобщение, позволяющее описать единым образом IPP-коды и IPP-системы множеств, предлагается в [7].

В § 2 мы дадим определение IPP-схемы в максимально возможной общности, опирающееся на совершенные схемы разделения секрета для произвольной монотонной структуры доступа, а также предложим критерий эффективности таких схем. Оставшаяся часть статьи посвящена обзору известных результатов про IPP-коды и IPP-системы множеств и формулировке открытых проблем.

§ 2. Общая постановка задачи

Рассмотрим произвольную *монотонную* структуру доступа, т.е. множество Γ подмножеств конечного множества $\mathcal{X}$ мощности n, обладающего тем свойством, что из $A \in \Gamma$ и $A \subset B$ следует, что $B \in \Gamma$. Множества A из Γ будем называть *разрешенными*. Имеется множество секретов S_0 с заданным распределением вероятностей $p(s_0)$ появления секрета $s_0 \in S_0$. Дистрибьютор выбирает множества "долей" секретов $S_1, \ldots, S_n$ и для каждого $s_0 \in S_0$ также выбирает некоторое распределение вероятностей $P_{s_0}(\boldsymbol{v}) = P_{s_0}(v_1, \ldots, v_n)$ на $V = S_1 \times \ldots \times S_n$. Чтобы распределить секрет s_0 дистрибьютор посылает с вероятностью $P_{s_0}(v_1, \ldots, v_n)$ символы $v_1, \ldots, v_n$ пользователям $1, 2, \ldots, n$ соответственно. При этом ℓ-й пользователь знает только долю-символ v_ℓ, который был послан ему, а остальные символы-доли ему неизвестны. Это называется схемой разделения секрета. Схема разделения секрета называется *совершенной* (ССРС), если, с одной стороны, участники из разрешенного множества (коалиции) $A \in \Gamma$ могут однозначно восстановить секрет s_0, т.е.

$\Pr(s_0 = \alpha_0 \,|\, s_i = \alpha_i,\ i \in A) \in \{0, 1\}$ для любого $A \in \Gamma$, а с другой стороны, участники неразрешенного множества $\widehat{A}$ не могут получить никакой дополнительной (апостериорной) информации о значении секрета из знания его долей, известных участникам $\widehat{A}$, т.е. $\Pr(s_0 = \alpha_0 \,|\, s_i = \alpha_i,\ i \in \widehat{A}) = \Pr(s_0 = \alpha_0)$. Возможны и комбинаторные определения ССРС различной общности, подробнее см. [8].

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

$$s_1 + \ldots + s_n = s \mod N, \tag{1}$$

где $S_0 = \ldots = S_n = G$, G – конечная абелева группа, например, группа вычетов по некоторому модулю N, а $s_1, \ldots, s_{n-1}$ – случайные независимые величины, равномерно распределенные на G. С помощью такой простейшей схемы можно построить ССРС для любой монотонной структуры доступа. Для этого достаточно рассмотреть минимальные (по включению) разрешенные множества и для каждого из них реализовать простейшую пороговую ССРС, задаваемую соотношением (1). Недостаток такой реализации в том, что мощность алфавита для i-й доли будет в N_i раз больше, чем мощность алфавита секрета, где N_i – число вхождений i в минимальные разрешенные множества. Так как N_i в наихудшем случае растет экспоненциально по n, то размер доли секрета может быть в экспоненциальное число раз больше размера секрета (см. [9, 10]). В частности, размер секрета растет как $2^{nH(w/n)}$ для такой реализации пороговой (w, n)-структуры доступа, тогда как схемы Блейкли [2] и Шамира [3] являются *идеальными*, т.е. мощность алфавита доли равна мощности алфавита секрета. Размер алфавита долей будет ниже учтен в определении эффективной скорости IPP-схем.

Пусть имеется ССРС, реализующая структуру доступа $\Gamma \subset 2^{\mathcal{X}}$, с множеством S_0 значений секрета и множествами "долей" секретов $S_1, \ldots, S_n$ мощности $Q_0, Q_1, \ldots, Q_n$ соответственно. Определим t-IPP-схему таким образом, чтобы t-IPP-коды и t-IPP-системы множеств были ее частными случаями. А именно, дистрибьютор передает M пользователям файл x в зашифрованном виде как $y = F(x, s_0)$, где $F(\cdot, \cdot)$ – отображение шифрования, а $s_0 \in \mathcal{S}_0$ – секретный ключ, который меняется для передачи другого файла. Для того чтобы пользователи могли дешифровать y, дистрибьютор передает им секретный ключ s_0 следующим образом: сначала "делит" секрет s_0 на n долей $s_1, \ldots, s_n$ в соответствии с данной ССРС, затем создает q различных зашифрованных копий $\widehat{s}_{1j}, \ldots, \widehat{s}_{qj}$ для каждой доли s_j с помощью некоторого другого отображения шифрования $G(\cdot, \cdot)$, где $\widehat{s}_{ij} = G(s_j, k_{ij})$, а $K_j = \{k_{1j}, \ldots, k_{qj}\}$ – множество из q ключей, используемых для шифрования/дешифрования доли s_j. Также среди всего множества Γ разрешенных подмножеств дистрибьютор выделяет M подмножеств $A_1, \ldots, A_M$, которые взаимно-однозначно соответствуют пользователям системы. Перед началом передачи файлов ℓ-й пользователь получает от дистрибьютора свою персональную последовательность ключей (декодер) α_ℓ, состоящую из ключей для дешифрования долей из *разрешенного* множества $A_\ell \in \Gamma$, по одному ключу для каждой "доли" из A_ℓ. Поэтому любой легальный пользователь может сначала дешифровать все доли из A_ℓ, затем восстановить секрет s_0, а с его помощью дешировать и файл y.

Поскольку схема разделения секрета совершенная, а множество ключей K_j, используемых для шифрования доли s_j, лежит в очень большом множестве всех возможных ключей (скажем, двоичных слов длины $N > 100$) и неизвестно пользователям (так как D выбирает эти ключи из всего множества случайно), и поэтому вероятность угадывания ключа ничтожно мала, то мы предполагаем, что произвольная коалиция недобросовестных пользователей, создавая ложное устройство для дешифрования файлов (декодер), должна предоставить этому устройству такой набор ключей из имеющихся в распоряжении коалиции, что эти ключи поз-

воляют дешифровать все доли из некоторого разрешенного множества. Занумеруем ключи в множествах K_j элементами q-ичного алфавита $\{1,\dots,q\}$ и сопоставим персональной последовательности ключей α_ℓ, предоставленной ℓ-му пользователю, $(q+1)$-ичный вектор c_ℓ с координатами из алфавита $\mathbb{Z}_{q+1}=\{0,1,\dots,q\}$, где j-я координата равна 0, если у пользователя нет ключа для j-й доли секрета. Далее мы будем отождествлять пользователя и сопоставляемый ему $(q+1)$-ичный вектор длины n.

Будем рассматривать множество векторов, сопоставленных M пользователям, как $(q+1)$-ичный код C длины n и мощности M. Пусть коалиция $U\subset C$ создала ложный декодер и ему соответствует вектор $\boldsymbol{z}=(z_1,\dots,z_n)\in\mathbb{Z}_{q+1}$, такой что $z_j\in U_j\cup 0$ для всех $j=1,\dots,n$, так как ложный декодер состоит только из ключей, принадлежащих участникам коалиции. Кроме того, $\operatorname{supp}(\boldsymbol{z})\in\Gamma$, так как для функционирования декодера необходимо, чтобы ключи декодера соответствовали какому-нибудь разрешенному множеству из Γ, где $\operatorname{supp}(\boldsymbol{z})=\{j:\ z_j\neq 0\}$. Таким образом, коалиция U может создать множество векторов

$$\langle U\rangle_\Gamma:=\{\boldsymbol{z}=(z_1,\dots,z_n)\in\mathbb{Z}_{q+1}:\ z_j\in U_j\cup 0,\ \operatorname{supp}(\boldsymbol{z})\in\Gamma\}. \tag{2}$$

Пара, состоящая из кода C и СРСР Γ, называется t-IPP-схемой, если по любому ложному декодеру, созданному коалицией U из не более чем t пользователей, хотя бы один из пользователей может быть безошибочно найден.

Определение 1. Пара (C,Γ), состоящая из $(q+1)$-ичного кода C длины n и СРСР, реализующей структуру доступа Γ, называется t-IPP-схемой, если для любого $\boldsymbol{z}\in\mathbb{Z}_{q+1}^n$ либо

$$\bigcap_{U\colon U\subset C,\,|U|\leqslant t,\,\boldsymbol{z}\in\langle U\rangle_\Gamma} U\neq\varnothing, \tag{3}$$

либо не существует коалиции $U\subset C$, такой что $|U|\leqslant t$ и $\boldsymbol{z}\in\langle U\rangle_\Gamma$.

Для пороговых схем разделения секрета это определение совпадает с определением, данным в [7], что, в свою очередь, означает, что известные ранее понятия t-IPP-кода и t-IPP-системы множеств являются частными случаями введенного понятия t-IPP-схемы.

Перейдем теперь к оценке эффективности t-IPP-схем. Воспользуемся следующим подходом, предложенным по существу уже в [1] и развитым в [11]. Естественным параметром, характеризующим эффективность кода, является его скорость, т.е. отношение логарифма мощности кода к его длине. В нашем случае нужно правильно определить "длину" IPP-схемы. Мы отмечали выше, что уже в [1] задача широковещательной передачи зашифрованного файла $y=F(x,s_0)$ была сведена к задаче широковещательной передачи секрета s_0. Тем самым, дистрибьютор передает M пользователям секрет s_0, и эффективностью такого способа передачи следует считать отношение "объема" переданной информации, т.е. $\log_2 M\times\log_2|S_0|$, к длине переданного сообщения, т.е. к $q\log_2(|S_1|\times\ldots\times|S_n|)$. Итак, мы определяем эффективную скорость R_{eff} t-IPP-схемы как

$$R_{\text{eff}}=\frac{\log_2|S_0|}{q\log_2(|S_1|\times\ldots\times|S_n|)}\log_2 M. \tag{4}$$

Хорошо известно, что у СССР $|S_j|\geqslant|S_0|$ для всех j. Также очевидно, что $M\leqslant q^n$. Поэтому брать очень большое q невыгодно, так как

$$R_{\text{eff}}\leqslant\frac{\log_2 q}{q}, \tag{5}$$

и следовательно, эффективная скорость стремится к нулю при росте q.

Для идеальных ССРС, к которым относятся и пороговые схемы, $|S_j| = |S_0|$ для всех j, и формула (4) превращается в

$$R_{\text{eff}} = \frac{\log_2 M}{qn} = q^{-1} R_2(C), \tag{6}$$

где $R_2(C) = n^{-1} \log_2 M$ – обычная двоичная скорость кода C.

§ 3. IPP-коды

Рассмотрим самый простой случай ССРС – (n, n)-пороговую схему, задаваемую соотношением (1), и возникающую IPP-схему, известную как IPP-коды [1,4]. Прежде всего отметим, что Γ состоит из всего одного множества – самого множества $\mathcal{X}$, и поэтому у произвольного ложного декодера-вектора $\boldsymbol{z} = (z_1, \ldots, z_n) \in \mathbb{Z}_{q+1}$ все координаты ненулевые. Обозначим $\mathcal{A}_q = \{1, 2, \ldots, q\}$. Тогда общее определение IPP-схемы видоизменяется следующим образом. Рассматривается произвольный q-ичный код C над алфавитом $\mathcal{A}_q$. В соответствии с (8) коалиция $U \subset C$ может создать множество векторов

$$\langle U \rangle := \{\boldsymbol{z} = (z_1, \ldots, z_n) \in \mathcal{A}_q : \; z_j \in U_j\}, \tag{7}$$

где $U_j = \{u_j : \; u \in U\}$. Будем называть множество $\langle U \rangle$ оболочкой множества U. Условие (7) отражает тот факт, что поддельный декодер $\boldsymbol{z}$ может состоять только из ключей, принадлежащих участникам коалиции.

Теперь определение t-IPP-схемы превращается в определение q-ичного t-IPP-кода.

О п р е д е л е н и е 2 [4]. Код $C \subset \mathcal{A}_q^n$ называется q-ичным t-IPP-кодом, если для любого $\boldsymbol{z} \in \mathcal{A}_q^n$ либо

$$\bigcap_{U:\, U \subset C,\, |U| \leqslant t,\, \boldsymbol{z} \in \langle U \rangle} U \neq \varnothing, \tag{8}$$

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

Иначе говоря, произвольный ложный декодер может быть в принципе порожден несколькими коалициями, однако у всех этих коалиций есть как минимум один общий участник, что и позволяет t-IPP-коду гарантированно найти хотя бы одного члена коалиции. Очевидно, что любой t-IPP-код является одновременно (t, t)-разделяющим кодом и $(t + 1)$-хэш-кодом. Напомним, что код C является (t, t)-разделяющим, если для любых двух непересекающихся подмножеств кода $U, V \subset C$, $|U| \leqslant t$, $|V| \leqslant t$, существует координата i, такая что $U_i \cap V_i = \varnothing$ (см. [12, 13]), и код C называется L-хэш-кодом, если для любых различных L векторов кода существует координата, значения в которой различны. Покажем, что из свойства t-IPP следует (t, t)-разделимость. Рассмотрим два произвольных непересекающихся подмножества $U, V \subset C$, $|U| \leqslant t$, $|V| \leqslant t$, t-IPP-кода C, и пусть их пересечения $U_i \cap V_i$ непусты для всех i. Выберем z_i так, что $z_i \in U_i \cap V_i$. Тогда вектор $\boldsymbol{z} = (z_1, \ldots, z_n)$ принадлежит и $\langle U \rangle$, и $\langle V \rangle$, но при этом U и V не пересекаются, что противоречит условию (8). Ниже мы воспользуемся этим свойством разделимости и известными верхними границами для мощности (t, t)-разделяющих кодов, чтобы получить верхнюю границу для мощности t-IPP-кодов.

Теперь покажем, что из свойства t-IPP следует свойство $(t + 1)$-хэш. Действительно, пусть это не так и в t-IPP-коде C существует подмножество U, такое что $|U_i| \leqslant t$ для всех i и $|U| = t + 1$. Так как $|U_i| \leqslant t$, то положим $z_i = \beta_i$, где β_i – значение, которое встречается в i-й координате в векторах множества U как минимум

дважды. Тогда вектор $\boldsymbol{z} = (z_1, \ldots, z_n)$ может быть порожден любым t-элементным подмножеством U, но пересечение этих подмножеств пусто. Заметим, что из свойства кода быть $(t+1)$-хэш-кодом немедленно следует, что при $q \leqslant t$ мощность любого t-IPP-кода не более t, но коды с такой мощностью тривиальны. Поэтому не существует нетривиальных q-ичных t-IPP-кодов для $q \leqslant t$, и в частности, не существует нетривиальных двоичных IPP-кодов. Ниже мы предполагаем, что $q > t$.

Более всего нас будут интересовать семейства так называемых хороших кодов, т.е. кодов, скорость которых отделена от нуля, где для кода длины n и мощности M его *скорость* (двоичная) определяется как $R = n^{-1} \log_2 M$. Пусть $M_q(n,t)$ – максимально возможная мощность q-ичного t-IPP-кода длины n. Тогда наибольшая возможная скорость q-ичного t-IPP-кода длины n – это

$$R_q(n,t) := n^{-1} \log_2 M_q(n,t). \tag{9}$$

Нас будут интересовать нижние границы на величину

$$R_*(q,t) := \liminf_{n\to\infty} R_q(n,t) \tag{10}$$

и верхние границы на величину

$$R^*(q,t) := \limsup_{n\to\infty} R_q(n,t). \tag{11}$$

В случае $t = 2$, т.е. коалиций из двух участников, свойства t-IPP-кода быть (t,t)-разделяющим кодом и $(t+1)$-хэш-кодом оказываются не только необходимыми, но и достаточными [4]. Отсюда из уже известных нижних границ для разделяющих и хэш-кодов (см. [12, 14]) следует следующая асимптотическая граница:

$$R_*(q,2) \geqslant \log_2 q - \frac{1}{3}\log_2(4q^2 - 6q + 3), \tag{12}$$

которая была доказана в [4] непосредственно, методом случайного кодирования. Там же была доказана верхняя граница $M_q(n,t) \leqslant 3q^{\lceil n/3 \rceil}$, из которой вытекает следующая верхняя асимптотическая граница:

$$R^*(q,2) \leqslant \frac{1}{3}\log_2 q, \tag{13}$$

которая вместе с границей (12) показывает, что при больших q скорость наилучших 2-IPP-кодов ведет себя как $\frac{1}{3}\log_2 q$. Но это кодовая скорость, которая для рассматриваемой задачи не так важна, как эффективная скорость R_{eff}. Максимум соответствующей нижней границы для R_{eff} равен 0,0536 и достигается при $q = 7$.

В случае размера коалиции $t > 2$ и $q > t^2$ существование хороших t-IPP-кодов было доказано еще в [1], основываясь на том замечании, что если у кода "большое" минимальное расстояние Хэмминга, то он является t-IPP-кодом. Более того, коды с большим расстоянием обладают тем свойством, что для любого вектора z ближайшее к нему (в метрике Хэмминга) кодовое слово принадлежит всем коалициям $U \subset C$ мощности не более t, способным генерировать z. Следуя [15], коды с таким свойством будем называть *t-идентифицирующими по минимуму расстояния кодами*, сокращенно – *t-MP-идентифицирующими кодами* (в англоязычной литературе – t-traceability codes). Дадим формальное определение.

Определение 3. Код C называется t-MP-идентифицирующим кодом, если для любой коалиции $U \subset C$, такой что $|U| \leqslant t$, любого вектора $\boldsymbol{z} \in \langle U \rangle$ и любого $\boldsymbol{c} \in C \setminus U$ справедливо

$$d(\boldsymbol{c}, \boldsymbol{z}) > \min_{u\in U} d(\boldsymbol{u}, \boldsymbol{z}). \tag{14}$$

Следующее утверждение дает количественную оценку понятию “большое” расстояние.

Лемма 1 [1]. *q-ичный код C длины n с кодовым расстоянием*

$$d(C) > n(1 - t^{-2}) \tag{15}$$

является t-MP-идентифицирующим кодом.

Доказательство. Для доказательства удобнее пользоваться не расстоянием Хэмминга $d(\boldsymbol{a}, \boldsymbol{b})$, а функцией “схожести”, определяемой как

$$S(\boldsymbol{a}, \boldsymbol{b}) := |\{i : \ a_i = b_i\}| = n - d(\boldsymbol{a}, \boldsymbol{b}).$$

Покажем, что для произвольной коалиции $U \subset C$, любого вектора $\boldsymbol{z} \in \langle U \rangle$, порожденного этой коалицией, и любого кодового вектора $\boldsymbol{c} \in C \setminus U$ не из коалиции справедливо неравенство

$$\max_{\boldsymbol{u} \in U} S(\boldsymbol{u}, \boldsymbol{z}) > S(\boldsymbol{z}, \boldsymbol{c}). \tag{16}$$

Действительно, с одной стороны,

$$\sum_{\boldsymbol{u} \in U} S(\boldsymbol{u}, \boldsymbol{z}) \geqslant n,$$

и следовательно,

$$\max_{\boldsymbol{u} \in U} S(\boldsymbol{u}, \boldsymbol{z}) \geqslant t^{-1} n.$$

С другой стороны,

$$S(\boldsymbol{c}, \boldsymbol{z}) \leqslant \sum_{\boldsymbol{u} \in U} S(\boldsymbol{c}, \boldsymbol{u}) < t \times n/t^2,$$

где последнее неравенство следует из условия (15). ▲

Очевидно, что t-MP-идентифицирующий код не просто является t-IPP-кодом, но сложность алгоритма поиска участника коалиции (“декодирование”) для t-MP-идентифицирующего кода имеет порядок M вместо M^t для обычных t-IPP-кодов.

Примером кодов с большим расстоянием и эффективным алгоритмом декодирования являются коды Рида – Соломона. В общем случае условие идентификации по минимуму расстояния (14) является более ограничительным, чем просто свойство IPP (8), однако для широкого класса кодов Рида – Соломона эти свойства эквивалентны [16].

Из обычной границы Варшамова – Гилберта для q-ичных кодов следует существование при $q > t^2$ хороших кодов, удовлетворяющих неравенству (15), т.е. кодов со свойством t-MP-идентифицирующего кода, следовательно, являющихся t-IPP-кодами. С другой стороны, из границы Плоткина следует, что при $q \leqslant t^2$ не существует хороших кодов, удовлетворяющих (15). Это в неявном виде было известно уже в работе [1], и довольно долго оставался открытым вопрос о существовании хороших t-IPP-кодов для всех $q \in [t + 1, t^2]$. Основная трудность этого случая заключается в том, что для $t > 2$ свойство t-IPP не получается так же просто переформулировать, как это было сделано в [4] для $t = 2$. Пример такого переформулирования для $t = 3$ на языке свойств типа разделимости можно найти в [17], и его сложность показывает, что такое разумное описание для произвольного t, по-видимому, невозможно. Поэтому в [17] было предложено достаточное условие с помощью введенного там же понятия частичного хэш-кода.

Код C называется (t,u)-частичным хэш-кодом, если для любых подмножеств T,U, таких что $T \subseteq U \subseteq C$, $|T| = t$, $|U| = u$, существует координата i, такая что $a_i \neq b_i$ для всех $\boldsymbol{a} \in T$ и всех $\boldsymbol{b} \in U \setminus T$. В [17] доказано, что (t,u)-*частичный хэш-код при* $u = \lfloor (t/2+1)^2 \rfloor$ *является* t-*IPP-кодом.* Основываясь на этом результате, в [17] было доказано существование для любого $q > t$ семейств t-IPP-кодов со скоростью, отделенной от нуля. Численное улучшение асимптотики было получено в [18], что дало, например, в частном случае $q = t+1$ существование t-IPP-кодов со скоростью $R \geqslant t^{-t+o(1)}$. Получаемые коды имеют экспоненциально малую по t скорость, тогда как даже идентифицирующие коды при $q > 2t^2$ имеют скорость порядка t^{-2}, правда, при большем q. Однако t-IPP-коды при $q = t(1+o(1))$ и не могут иметь большую скорость, как следует из известных границ для (t,t)-разделяющих кодов. Действительно, в [19] доказана следующая верхняя граница на скорость $R_{\mathrm{sep}}(q,t)$ (t,t)-разделяющих кодов:

$$R_{\mathrm{sep}}(q,t) \leqslant c\frac{2^q}{2^{2t}\log_2 q}(1+o(1)), \tag{17}$$

где $c < 2{,}1$, из которой следует, что

$$R^*(t+1,t) \leqslant 2^{-t(1+o(1))},$$

и скорость t-IPP-кодов экспоненциально мала по t при $q = t+1$. Тем более, экспоненциально мала эффективная скорость таких кодов.

С другой стороны, q-ичные коды, лежащие на границе Варшамова – Гилберта и удовлетворяющие неравенству (15), являются t-IPP-кодами (и даже с дополнительным свойством t-MP-идентификации), и их эффективная скорость имеет порядок t^{-4}, например, при $q = 2t^2$. Истинный порядок максимальной эффективной скорости при наилучшем выборе q для t-IPP-кодов и t-MP-идентифицирующих кодов неизвестен.

Другой вопрос, также связанный с существованием хороших кодов при минимальном значении q, выглядит следующим образом: *каков минимальный размер алфавита* q_t, *для которого существуют хорошие* t-*MP-идентифицирующие коды*? Известно [15], что $q_2 = 3$, а для больших значений параметра t в [20] было доказано, что

$$q_t \leqslant t^2 - \left\lceil \frac{t}{2} \right\rceil + 1,$$

что несколько улучшает очевидную границу $q_t \leqslant t^2 + 1$. Первый открытый случай – это значение q_3.

§ 4. IPP-системы множеств

Рассмотрим второй известный частный случай IPP-схем, введенный в [5, 6] под названием *IPP-системы множеств* (IPP-set systems в англоязычной литературе). IPP-системы множеств основываются на общих пороговых (w,n)-схемах разделения секрета [2, 3], в которых w или более долей секрета достаточно для однозначного нахождения секрета, а меньшее число долей не дает никакой дополнительной (апостериорной) информации о секрете. Дадим формальное определение IPP-системы множеств как частного случая IPP-схем.

Структура доступа описывается как

$$\Gamma_w = \{A \subseteq \mathcal{X} : |A| \geqslant w\},$$

т.е. это всевозможные подмножества мощности по крайней мере w. В данной модели у дистрибьютора имеется множество $\mathcal{X}$ из n ключей шифрования, с помощью кото-

рых он шифрует доли секрета – каждую на своем ключе, т.е. $q = 1$. Декодер для ℓ-го пользователя – это двоичный вектор $\boldsymbol{c}_\ell$ веса Хэмминга $\mathrm{wt}(\boldsymbol{c}_\ell) = w$, и множество векторов, ассоциированных с пользователями, образует двоичный равновесный код C веса w. Коалиция $U \subset C$ может создать множество векторов

$$\langle U\rangle_{\mathrm{set}} = \{\boldsymbol{z} \in \{0,1\}^n : \ z_i \in U_i \cup \{0\} \text{ и } \mathrm{wt}(\boldsymbol{z}) \geqslant w\},$$

что соответствует общему определению (2). Отметим различие в моделях IPP-систем множеств и IPP-кодов: коалиция из равновесных векторов веса w может ставить символ 0 и в тех позициях, где у всех векторов коалиции стоит символ 1 (если при этом общее число единиц в результирующем векторе будет не менее w), тогда как для IPP-кодов это невозможно (см. (7)). Следуя общему определению 1, получаем определение IPP-системы множеств как двоичного равновесного кода.

Определение 4. Двоичный равновесный код $C = \{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_M\} \subset \{0,1\}^n$ веса w называется (t, w)-IPP-кодом, если для любого $\boldsymbol{z} \in \{0,1\}^n$, $\mathrm{wt}(\boldsymbol{z}) \geqslant w$, либо справедливо

$$\bigcap_{U\subset C:\, \boldsymbol{z}\in\langle U\rangle_{\mathrm{set}},\, |U|\leqslant t} U \neq \varnothing, \tag{18}$$

либо нет кодовой коалиции из не более чем t участников, которая могла бы породить $\boldsymbol{z}$.

Это определение легко трансформировать в первоначальное определение t-IPP-системы множеств.

Определение 5 [6]. Семейство $\boldsymbol{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_M\}$ w-подмножеств множества $\mathcal{X}$ называется (t, w)-IPP-системой множеств, если для любого $Z \subset \mathcal{X}$, такого что $|Z| \geqslant w$, либо

$$\bigcap_{U\subset \boldsymbol{F}:\, Z\in\langle U\rangle_{\mathrm{set}},\, |U|\leqslant t} U \neq \varnothing, \tag{19}$$

либо нет коалиции $U \subset \boldsymbol{F}$, такой что $|U| \leqslant t$ и $Z \in \langle U\rangle_{\mathrm{set}}$.

Другими словами, семейство $\boldsymbol{F}$, состоящее из некоторых w-подмножеств множества $\{1, \ldots, n\}$, является (t, w)-IPP-системой множеств, если для любого ($\geqslant w$)-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, из определения следует, что никакой элемент из $\boldsymbol{F}$ не принадлежит объединению t других множеств из $\boldsymbol{F}$. Такие семейства известны как семейства множеств без перекрытия (cover-free sets) [21, 22]. Характеристические векторы этих множеств задают так называемый *дизъюнктивный код* (см. [23, 24]). Напомним, что двоичный код C называется t-дизъюнктивным, если для любого подмножества $U \subset C$, $|U| \leqslant t$, и любого кодового вектора $\boldsymbol{c} \in C$ из равенства

$$\bigvee_{\boldsymbol{u}\in U} \boldsymbol{u} = \boldsymbol{c} \vee \Big(\bigvee_{\boldsymbol{u}\in U} \boldsymbol{u}\Big)$$

следует $\boldsymbol{c} \in U$.

Заметим, что в работе [5], в которой впервые было введено понятие (w, n)-систем множеств, рассматриваются системы множеств с дополнительным свойством, аналогичным свойству идентификации по минимуму расстояния для IPP-кодов. В терминах систем множеств это свойство означает, что участник коалиции может быть найден как пользователь, имеющий максимальную мощность пересечения с поддельным множеством (декодером). Дадим формальное определение.

Определение 6. Семейство $\boldsymbol{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_M\}$ w-подмножеств множества $\{1, \ldots, n\}$ называется (t, w)-МР-идентифицирующей системой множеств, если для любой коалиции U, такой что $|U| \leqslant t$, любого множества $Z \in \langle U \rangle_{\text{set}}$ и любого $j \notin U$ выполняется неравенство

$$|Z \cap \mathcal{F}_j| < \max_{u \in U} |Z \cap \mathcal{F}_u|. \tag{20}$$

Следующая лемма, аналогичная лемме 1, дает простое достаточное условие для семейства множеств быть (t, w)-МР-идентифицирующей системой множеств.

Лемма 2. *Семейство $\boldsymbol{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_M\}$ w-подмножеств множества $\mathcal{X}$, такое что $|\mathcal{F}_i \cap \mathcal{F}_j| < w/t^2$ для любых $\mathcal{F}_i, \mathcal{F}_j \in \boldsymbol{F}$, $i \neq j$, является (t, w)-МР-идентифицирующей системой множеств.*

Двоичный равновесный код, соответствующий (t, w)-МР-идентифицирующей системе множеств, будем называть (t, w)-МР-идентифицирующим кодом. Определение 6 и лемма 2 могут быть переформулированы следующим образом.

Определение 7. Двоичный равновесный код C веса w называется (t, w)-МР-идентифицирующим кодом, если для любой коалиции $U \subset C$, $|U| \leqslant t$, любого вектора $\boldsymbol{z} \in \langle U \rangle_{\text{set}}$ и любого $\boldsymbol{c} \in C \setminus U$ выполняется неравенство

$$d(\boldsymbol{z}, \boldsymbol{c}) > \min_{u \in U} d(\boldsymbol{z}, \boldsymbol{u}). \tag{21}$$

Лемма 3. *Если для минимального расстояния двоичного равновесного кода C веса w справедливо неравенство*

$$d(C) > 2w(1 - t^{-2}), \tag{22}$$

то C является (t, w)-МР-идентифицирующим кодом.

Из последней леммы и аналога границы Варшамова – Гилберта для равновесных кодов (см. [25]) следует существование (t, w)-МР-идентифицирующих кодов с асимптотической скоростью [11]

$$R_t^{MD}(\omega) \geqslant H(\omega) - \omega H\Big(\frac{\tau}{\omega}\Big) - (1 - \omega) H\Big(\frac{\tau}{1 - \omega}\Big), \tag{23}$$

где

$$H(x) = -(x \log_2 x + (1 - x) \log_2 (1 - x))$$

– функция двоичной энтропии, $\tau = \omega(1 - 1/t^2)$ и $\omega < t^{-2}$. Подставив в (23) значение $\omega = 0{,}5t^{-2}$, получим существование (t, w)-МР-идентифицирующих кодов с асимптотической скоростью R_t^{MD} порядка $c' t^{-4}$, где $c' > 0{,}5$. С другой стороны, благодаря замечательному результату, доказанному в [26], что произвольный (t, w)-МР-идентифицирующий код является t^2-дизъюнктивным кодом, и известным верхним границам [22, 24], гласящим, что скорость t-дизъюнктивного кода имеет порядок $O(t^{-2} \log t)$, получаем

$$R_t^{MD} \leqslant O(t^{-4} \log t).$$

Следовательно, о наилучших (t, w)-МР-идентифицирующих кодах мы знаем, что их скорость R_t^{MD} асимптотически ведет себя при больших t как t^{-4} с точностью до мультипликативного множителя не более $(\log t)^2$. Тем самым, при больших t

$$R_t^{MD} = t^{-4 + o(1)}. \tag{24}$$

Для произвольных (t, w)-IPP-кодов известная нижняя граница ведет себя так же, как и для (t, w)-МР-идентифицирующих кодов, т.е. имеет порядок t^{-4}, а вот

известные верхние границы намного слабее (см. [6]). В результате для (t, w)-IPP-кодов неизвестен даже полиномиальный порядок скорости, как, впрочем, и для t-IPP-кодов.

§ 5. Заключение

В данной статье мы предложили новую, максимально общую модель "кодов" с идентификацией "родителей", которую мы назвали IPP-схемами. Мы надеемся, что эта модель позволит не только унифицированно описывать известные ранее модели, как то: IPP-коды и IPP-системы множеств, но и даст ответ на наиболее важный открытый вопрос в данной области – найти асимптотику скорости наилучших IPP-схем как функции от размера t коалиций недобросовестных пользователей. Как первый шаг в этом направлении надо найти полиномиальный (по t) порядок скорости, как это удалось сделать для систем множеств с идентификацией по минимуму расстояния, ср. (24).

Мы рассматривали семейства кодов и множеств со свойством t-IPP и максимально возможной скоростью и интересовались асимптотикой скорости, когда размер алфавита q фиксирован, а длина кода растет, что довольно типично для теории кодирования. Результаты, касающиеся "обратного" процесса, т.е. когда длина кода фиксирована, а размер алфавита q растет, представляют не меньший интерес. Их частично можно найти в обзоре [27] (см. также работу [26] и ссылки в ней).

Мы отдельно рассматривали IPP-коды со свойством идентификации по минимуму расстояния и, что эквивалентно, IPP-семейства множеств с идентификацией по максимуму пересечения. Это свойство очевидным образом сокращает сложность с $O(M^t)$ для общего случая до $O(M)$, но сложность все равно экспоненциальна по n. В [28] было построено семейство IPP-кодов с алгоритмом идентификации (участника коалиции) полиномиальной по n сложности. Класс (t, w)-MP-идентифицирующих кодов (или семейств множеств) с полиномиальным алгоритмом идентификации был построен в [29]. Обе конструкции основываются на каскадной конструкции с алгеброгеометрическим кодом [30] в качестве внешнего кода и "мягким" алгоритмом Гурусвами – Судана декодирования каскадных кодов (см. [31]). Для построения двоичных равновесных кодов с полиномиальным алгоритмом идентификации использовалась каскадная конструкция из работ [23, 32], где в качестве внутреннего кода берется множество из Q двоичных векторов длины Q и веса 1.

Как отмечалось в § 3, так как t-IPP-код является $(t + 1)$-хэш-кодом, то не существует нетривиальных двоичных t-IPP-кодов. Это послужило одной из причин рассмотрения так называемых кодов цифровых отпечатков пальцев, устойчивых к коалиционным атакам (collusion-secure digital fingerptinting в англоязычной литературе) [33]. Основное отличие кодов цифровых отпечатков пальцев от IPP-кодов заключается в том, что идентификация участника коалиции недобросовестных пользователей допускается с *ненулевой вероятностью ошибки*. На самом деле, код цифровых отпечатков пальцев – это не один код, а целое семейство кодов, где конкретный код выбирается случайно, с некоторым заданным распределением вероятностей. Только дистрибьютор знает, какой конкретный код из семейства был выбран, что позволяет добиваться, при правильном построении семейства кодов, стремления к нулю вероятности ошибочной идентификации с ростом длины кодов [33–35]. Стремление к нулю вероятности ошибки делает правдоподобным общепринятое суждение, что коды цифровых отпечатков пальцев – это почти IPP-коды, и что они удовлетворяют требованию, сформулированному еще в [1]: "возможность безошибочного (или с минимально возможной вероятностью) обнаружения источника пиратства *с предоставлением неопровержимого доказательства*". Действительно, для коалиций из двух участников было доказано существование хороших (со скоростью, отделенной от нуля) кодов со свойством "почти" IPP [36], т.е. свойство (8) для таких кодов почти

всегда будет выполнено. Однако, как было показано в [37], для коалиций из трех и более участников хорошие "почти" IPP-коды не существуют, т.е. свойство (8) будет почти всегда не выполнено, какое бы семейство кодов мы ни выбрали. Поэтому было предложено заменить свойство (8) на более слабое, когда алгоритм идентификации должен выдавать не одного пользователя, а список подозрительных пользователей, такой что как минимум один из списка принадлежит коалиции [37]. Но это уже новая, мало исследованная постановка задачи, выходящая за рамки настоящей статьи.

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. *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.
3. *Shamir A.* How to Share a Secret // Comm. ACM. 1979. V. 22. № 11. P. 612–613.
4. *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.
5. *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.
6. *Collins M.J.* Upper Bounds for Parent-Identifying Set Systems // Des. Codes Cryptogr. 2009. V. 51. № 2. P. 167–173.
7. *Егорова Е.Е.* Обобщение IPP-кодов и IPP-систем множеств // Пробл. передачи информ. 2019. Т. 55. № 3. С. 46–59.
8. *Блейкли Р.Г., Кабатянский Г.А.* Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Пробл. передачи информ. 1997. Т. 33. № 3. P. 102–110.
9. *Benaloh J., Leichter J.* Generalized Secret Sharing and Monotone Functions // Advances in Cryptology—CRYPTO'88 (Proc. 8th Annual Int. Cryptology Conf. Santa Barbara, CA, USA. August 21–25, 1988). Lect. Notes Comp. Sci. V. 403. Berlin: Springer, 1990. P. 27–35.
10. *Ito M., Saito A., Nishizeki T.* Secret Sharing Scheme Realizing General Access Structure // Electron. Comm. Japan Part III Fund. Electron. Sci. 1989. V. 72. № 9. P. 56–63.
11. *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.
12. *Сагалович Ю.Л.* Разделяющие системы // Пробл. передачи информ. 1994. Т. 30. № 2. С. 14–35.
13. *Cohen G.D., Schaathun H.G.* Asymptotic Overview on Separating Codes // Tech. Rep. № 248. Dept. of Informatics, Univ. of Bergen. Bergen, Norway, 2003.
14. *Bassalygo L.A., Burmester M., Dyachkov A., Kabatianskii G.* Hash Codes // Proc. 1997 IEEE Int. Sympos. on Information Theory (ISIT'97). Ulm, Germany. June 29 – July 4, 1997. P. 174.
15. *Кабатянский Г.А.* Коды для защиты авторских прав: случай двух пиратов // Пробл. передачи информ. 2005. Т. 41. № 2. С. 123–127.
16. *Fernandez M., Cotrina J., Soriano M., Domingo N.* A Note about the Identifier Parent Property in Reed–Solomon Codes // Comput. Secur. 2010. V. 29. № 5. P. 628–635.
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. *Воробьев И.В.* Границы скоростей разделяющих кодов // Пробл. передачи информ. 2017. Т. 53. № 1. С. 34–46.

20. *Blackburn S.R., Etzion T., Ng S.-L.* Traceability Codes // J. Combin. Theory Ser. A. 2010. V. 117. № 8. P. 1049–1057.
21. *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.
22. *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.
23. *Kautz W.H., Singleton R.C.* Nonrandom Binary Superimposed Codes // IEEE Trans. Inform. Theory. 1964. V. 10. № 4. P. 363–377.
24. *Дьячков А.Г., Рыков В.В.* Границы длины дизъюнктивных кодов // Пробл. передачи информ. 1982. Т. 18. № 3. С. 7–13.
25. *Левенштейн В.И.* О верхних оценках для кодов с фиксированным весом векторов // Пробл. передачи информ. 1971. Т. 7. № 4. С. 3–12.
26. *Gu Y., Miao Y.* Bounds on Traceability Schemes // IEEE Trans. Inform. Theory. 2018. V. 64. № 5. P. 3450–3460.
27. *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.
28. *Barg A., Kabatiansky G.* A Class of I.P.P. Codes with Efficient Identification // J. Complexity. 2004. V. 20. № 2–3. P. 137–147.
29. *Egorova E., Fernandez M., Kabatiansky G.* A Construction of Traceability Set Systems with Polynomial Tracing Algorithm // Proc. 2019 IEEE Int. Sympos. on Information Theory (ISIT'2019). Paris, France. July 7–12, 2019 (to appear).
30. *Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А.* Алгеброгеометрические коды: Основные понятия. М.: МЦНМО, 2003.
31. *Guruswami V.* List Decoding of Error-Correcting Codes (Winning Thesis of the 2002 ACM Doct. Diss. Competition) // Lect. Notes Comp. Sci. V. 3282. Berlin: Springer, 2004.
32. *Ericson T., Zinoviev V.A.* An Improvement of the Gilbert Bound for Constant Weight Codes // IEEE Trans. Inform. Theory. 1987. V. 33. № 5. P. 721–723.
33. *Boneh D., Shaw J.* Collusion-Secure Fingerprinting for Digital Data // IEEE Trans. Inform. Theory. 1998. V. 44. № 5. P. 1897–1905.
34. *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.
35. *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.
36. *Fernandez M., Kabatiansky G., Moreira J.* Almost IPP-Codes or Provably Secure Digital Fingerprinting Codes // Proc. 2015 IEEE Int. Sympos. on Information Theory (ISIT'2015). Hong Kong, China. June 14–19, 2015. P. 1595–1599.
37. *Fernandez M., Egorova E., Kabatiansky G.* Binary Fingerprinting Codes — Can We Prove that Someone Is Guilty?! // Proc. 2015 IEEE Int. Workshop on Information Forensics and Security (WIFS'2015). Rome, Italy. November 16–19, 2015. P. 1–4.

Кабатянский Григорий Анатольевич
Сколковский институт науки и технологий
g.kabatyansky@skoltech.ru

Поступила в редакцию
08.04.2019
После доработки
08.04.2019
Принята к публикации
18.06.2019