Math-Net.Ru

Общероссийский математический портал

Ю. В. Косолапов, Схема разделения секрета типа схемы Блэкли, основанная на пересечении подпространств, *Матем. вопр. криптогр.*, 2017, том 8, выпуск 1, 13–30

DOI: <https://doi.org/10.4213/mvk212>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 34.239.49.27

26 апреля 2023 г., 15:39:11

**Схема разделения секрета типа схемы Блэкли,
основанная на пересечении подпространств**

Ю. В. Косолапов

Южный федеральный университет, Ростов-на-Дону

Получено 23.V.2016

Аннотация. Рассматривается задача построения схемы разделения секрета, в которой возможна замена любого подмножества участников новыми участниками; при этом доли секрета вычисляются только для новых участников, а доли секрета у незамененных участников остаются прежними. С помощью теории помехоустойчивых кодов строятся протоколы разделения и восстановления секрета. Для исследования допустимых границ параметров построенной схемы распределения секрета вводится и исследуется новая характеристика линейного кода. В качестве примеров приводятся реализации предложенной схемы на основе некоторых кодов.

Ключевые слова: схема разделения секрета, пересечение подпространств, линейный код

**Blakley type secret sharing scheme based on the intersection
of subspaces**

Yu. V. Kosolapov

Southern Federal University, Rostov-on-Don

Abstract. We consider the problem of constructing a secret sharing schemes permitting to replace any subset of participants with new participants so that new secret shares may be calculated only for the newly added members, and secret shares of others participants do not change. Using the theory of error-correcting codes we construct protocols of separation and recovery of the secret. In order to study the permissible domains of parameters of this secret sharing scheme the new characteristics of linear code is introduced and explored. We implement the proposed scheme for some linear codes as examples.

Key words: secret sharing scheme, subspace intersection, linear code

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 13–30 (Russian)

© Академия криптографии Российской Федерации, 2017 г.

1. Введение и постановка задачи

Схемы разделения секрета (СРС) применяются как самостоятельно, так и в качестве примитива при синтезе других криптографических протоколов, например протоколов многосторонних конфиденциальных вычислений (ПМКВ) [1, 2]. В частности, в [1] показано, что ПМКВ могут быть построены на основе любой линейной СРС. Здесь и далее, в соответствии с [2], под линейной СРС понимается следующая схема. Пусть $\mathbb{F} = \mathbb{F}_q$ — поле Галуа мощности q , $\mathbb{F}^k$ — пространство размерности k над полем $\mathbb{F}$, $k \in \mathbb{N}$, $\mathcal{P} = \{P_1, \dots, P_l\}$ — упорядоченное множество из l участников, $(s_1, \dots, s_l)$ — вектор долей секрета $s (s \in \mathbb{F}^k)$, $s_i \in \mathbb{F}^{p_i}$, $p_i \in \mathbb{N}$, полученных дилером в соответствии с протоколом разделения секрета (в работе используется терминология из [3], общепринятая для СРС). Схема разделения секрета называется *линейной*, если для любых секретов s и $\hat{s}$ из $\mathbb{F}^k$ и соответствующих векторов долей секретов $(s_1, \dots, s_l)$ и $(\hat{s}_1, \dots, \hat{s}_l)$ выполняется условие: векторы $(s_1 + \hat{s}_1, \dots, s_l + \hat{s}_l)$ и $(\lambda s_1, \dots, \lambda s_l)$ являются векторами долей секретов $s + \hat{s}$ и λs соответственно, $\lambda \in \mathbb{F}$. К линейным СРС, в частности, относятся классические схемы Шамира [4] и Блэкли [5], а также их обобщения из [6–8]. Протокол разделения секрета для линейной СРС в общем виде состоит в нахождении дилером для каждого $i \in \{1, \dots, l\}$ значения соответствующего (несекретного) отображения $f_i : \mathbb{F}^k \times \mathbb{F}^e \rightarrow \mathbb{F}^{p_i}$, где e — подходящее для конкретной СРС натуральное число. Именно, если s — секрет, то вектор долей секрета представим в виде

$$(f_1(s, a), f_2(s, a), \dots, f_l(s, a)),$$

где a — вектор, выбранный дилером из $\mathbb{F}^e$ случайно и равномерно. Отметим, что СРС называется *пороговой* (l, t) -схемой, если любые t и более участников образуют *правомочную коалицию*, т. е. могут восстановить секрет, а меньшие совокупности участников секрет восстановить не могут. Множество всех правомочных коалиций называется *структурой доступа*.

Заметим, что если $\hat{\mathcal{P}} = \{P_{i_1}, \dots, P_{i_u}\}$ — подмножество, состоящее из u ($u \leq l$) участников, которых необходимо заменить новыми u участниками, образующими подмножество $\hat{\mathcal{P}}' = \{P'_{i_1}, \dots, P'_{i_u}\}$, то процедуру замены можно реализовать двумя способами. Первый способ предполагает выполнение дилером заново протокола разделения секрета для обновленного множества участников $\mathcal{P}' = (\mathcal{P} \setminus \hat{\mathcal{P}}) \cup \hat{\mathcal{P}}'$ с использованием, возможно, нового значения случайного вектора a' . Тогда доли секрета передаются всем участникам множества $\mathcal{P}'$: как новым участникам из $\hat{\mathcal{P}}'$, так и незамененным участникам из $\mathcal{P}' \setminus \hat{\mathcal{P}}'$.

Особенностью этого способа является то, что обновление множества участников нельзя провести анонимно, т. е. без изменения долей секрета участников из $\mathcal{P}' \setminus \hat{\mathcal{P}}'$. Второй способ — вычисление долей секрета только для участников из $\hat{\mathcal{P}}'$, однако для реализации этого способа требуется хранение дилером вектора $\mathbf{a}$ вместе с $\mathbf{s}$.

В настоящей работе решается задача построения СРС, для которой замена любых $u (\leq l)$ участников проводится нахождением долей секрета только для u новых участников без изменения долей секрета у незамененных участников. Другими словами, для любого секрета $\mathbf{s} (\in \mathbb{F}^k)$ вектор долей секрета в СРС должен иметь вид

$$(f_1(\mathbf{s}, \mathbf{a}_1), f_2(\mathbf{s}, \mathbf{a}_2), \dots, f_l(\mathbf{s}, \mathbf{a}_l)), \quad (1)$$

где векторы $\mathbf{a}_1, \dots, \mathbf{a}_l$ выбираются из множества $\mathbb{F}^e$ случайно, равновероятно, независимо друг от друга и независимо от $\mathbf{s}$.

Работа имеет следующую структуру. Во втором разделе с применением теории помехоустойчивых кодов строится СРС, в основе алгоритма восстановления секрета которой лежит нахождение пересечения подпространств. Именно поэтому эта СРС названа в настоящей работе схемой типа схемы Блэкли, так как последняя строится на идее пересечения гиперплоскостей [5]. Также во втором разделе с целью исследования границ параметров предлагаемой в настоящей работе СРС для линейного $[n, k]$ -кода C вводится характеристика $I(C)$, описывающая для каждой пары $(i, j) \in \{0, \dots, k\} \times \{0, \dots, n\}$ минимальное количество наборов столбцов порождающей матрицы (каждый набор состоит из j столбцов), при котором размерность пересечения натянутых на эти наборы линейных оболочек не превышает i . Исследованию характеристики $I(C)$ посвящен третий раздел. Отметим, что результаты третьего раздела не привязаны к теории СРС, так как, по мнению автора, могут представлять самостоятельный интерес. В четвертом разделе на основе результатов предыдущих двух приводятся реализации СРС типа схемы Блэкли для конкретных кодов.

2. Схема разделения секрета типа схемы Блэкли

Пусть $\underline{n} = \{1, \dots, n\}$, $\underline{n}_0 = \underline{n} \cup \{0\}$, $\text{supp}(D) = \{i : \exists (x_1, \dots, x_n) \in D, x_i \neq 0\}$ — носитель множества $D (\subseteq \mathbb{F}^n)$, $C (\subseteq \mathbb{F}^n)$ — $[n, k, d]$ -код длины n , размерности k ($\dim(C) = k$) с кодовым расстоянием d и порождающей матрицей $G = (\mathbf{g}_i)_{i=1}^k$, где $\mathbf{g}_i$ — i -я строка матрицы G .

Для упорядоченного множества $S = \{s_1, \dots, s_h\} \subseteq \underline{n}$ (где $s_1 < s_2 < \dots < s_h$) рассмотрим оператор проекции $\dot{\pi}_S : \mathbb{F}^n \rightarrow \mathbb{F}^h$, действующий на вектор $\mathbf{x} = (x_1, \dots, x_n) (\in \mathbb{F}^n)$ по правилу: $\dot{\pi}_S(\mathbf{x}) = (x_{s_1}, \dots, x_{s_h}) (\in \mathbb{F}^h)$. Если $A = (\mathbf{a}_i)_{i=1}^u$ — матрица размера $u \times n$ (или $(u \times n)$ -матрица), то символом $\pi_S(A)$ обозначим матрицу $(\dot{\pi}_S(\mathbf{a}_i))_{i=1}^u$ и назовем ее проекцией матрицы A на множество S . Проекцией $[n, k, d]$ -кода C на множество $S (\subseteq \underline{n})$, $|S| = h$, назовем подпространство $\hat{\pi}_S(C)$ пространства $\mathbb{F}^h$, порожденное строками матрицы $\pi_S(G)$, $\dim(\hat{\pi}_S(C)) \leq h$. Линейную оболочку, порожденную столбцами матрицы $\pi_S(G)$, обозначим $\mathcal{L}_S(G)$; при этом будем писать $\mathcal{L}_S(G) \subseteq \mathbb{F}^k$, рассматривая $\mathbb{F}^k$ при таком написании как пространство вектор-столбцов размерности k . Отметим, что

$$\dim(\hat{\pi}_S(C)) = \dim(\mathcal{L}_S(G)) = \text{rank}(\pi_S(G)).$$

Пусть C — линейный $[n, k, d]$ -код, $\mathcal{T} = \{\tau_1, \dots, \tau_l\}$ — такой набор подмножеств $\tau_i \subseteq \underline{n}$, $i = 1, \dots, l$, что найдется хотя бы одно непустое множество $A \subseteq \underline{l}$, для которого выполняется равенство

$$\bigcap_{i \in A} \mathcal{L}_{\tau_i}(G) = \{\mathbf{0}\} (\in \mathbb{F}^k). \quad (2)$$

Каждому участнику $P_i (\in \mathcal{P} = \{P_1, \dots, P_l\})$ соответствует множество τ_i , причем это соответствие считается несекретным. Предлагается следующий протокол разделения секрета $\mathbf{s} (\in \mathbb{F}^k)$ среди l участников множества $\mathcal{P}$. Дилер выбирает порождающую матрицу G кода C и передает участнику P_i ($i = 1, \dots, l$) соответствующую долю секрета: вектор $\dot{\pi}_{\sigma_i}(\mathbf{c}_i)$, где $\sigma_i = \underline{n} \setminus \tau_i$, а $\mathbf{c}_i$ — случайно и равномерно выбранный дилером вектор из множества решений системы $G\mathbf{x}^\top = \mathbf{s}^\top$ относительно вектора неизвестных $\mathbf{x}$ (здесь и далее $A^\top$ обозначает транспонирование матрицы A). Мощность $|\sigma_i|$ множества σ_i будем называть длиной i -й доли секрета. Пусть $C^\perp$ — $[n, n - k]$ -код с порождающей матрицей $G^\perp$, ортогональный коду C , C' — такое подпространство размерности k , что прямая сумма $C' \oplus C^\perp$ совпадает с $\mathbb{F}^n$, а $\chi : \mathbb{F}^k \rightarrow C'$ — такой изоморфизм, что $G\chi(\mathbf{s})^\top = \mathbf{s}^\top$ для всех $\mathbf{s} \in \mathbb{F}^k$. Как несложно проверить, можно считать, что для каждого $i \in \underline{l}$ вектор $\mathbf{c}_i$ выбирается случайно и равномерно из смежного класса $\chi(\mathbf{s}) + C^\perp$ кода $C^\perp$. Другими словами, найдется такой вектор $\mathbf{a}_i (\in \mathbb{F}^{n-k})$, что

$$\mathbf{c}_i = \chi(\mathbf{s}) + \mathbf{a}_i G^\perp. \quad (3)$$

Отсюда следует, что отображение f_i (см. (1)) имеет вид $f_i(\mathbf{s}, \mathbf{a}_i) = \dot{\pi}_{\sigma_i}(\chi(\mathbf{s}) + \mathbf{a}_i G^\perp)$ для каждого $i \in \underline{l}$.

Заметим, что правило (3) фактически задает правило случайного кодирования, которое, в частности, применяется для защиты данных в каналах, допускающих подслушивание. В частности, в терминах модели частичного наблюдения, рассмотренной в [9], участник $P_i (i \in \underline{l})$ предлагаемой в настоящей работе СРС может рассматриваться как *наблюдатель*, которому известно $|\sigma_i|$ символов вектора $\mathbf{c}_i (\in \mathbb{F}^n)$, полученного по правилу (3). Тогда из [9] следует, что если априори участникам СРС неизвестна какая-либо информация о секрете $\mathbf{s}$, то i -й участник на основании своей доли секрета сможет построить множество N_{σ_i} претендентов на секрет, причем $|N_{\sigma_i}| = q^{\pi_{\sigma_i}(G)}$. Как доказано в [10], N_{σ_i} не зависит от используемого в (3) вектора $\mathbf{a}_i$. Коалиция участников с номерами из множества $\{i_1, \dots, i_v\} (\subseteq \underline{l})$ может сузить множество претендентов, построив пересечение соответствующих множеств: $\cap_{j=1}^v N_{\sigma_{i_j}}$. Для нахождения этого пересечения необходимо решить относительно неизвестного $\mathbf{s}$ систему

$$\begin{cases} \pi_{\sigma_{i_1}}(G)(\dot{\pi}_{\sigma_{i_1}}(\mathbf{c}_{i_1}))^\top + \pi_{\tau_{i_1}}(G)(\dot{\pi}_{\tau_{i_1}}(\mathbf{c}_{i_1}))^\top = \mathbf{s}^\top, \\ \pi_{\sigma_{i_2}}(G)(\dot{\pi}_{\sigma_{i_2}}(\mathbf{c}_{i_2}))^\top + \pi_{\tau_{i_2}}(G)(\dot{\pi}_{\tau_{i_2}}(\mathbf{c}_{i_2}))^\top = \mathbf{s}^\top, \\ \dots \\ \pi_{\sigma_{i_v}}(G)(\dot{\pi}_{\sigma_{i_v}}(\mathbf{c}_{i_v}))^\top + \pi_{\tau_{i_v}}(G)(\dot{\pi}_{\tau_{i_v}}(\mathbf{c}_{i_v}))^\top = \mathbf{s}^\top, \end{cases} \quad (4)$$

в которой известны $\dot{\pi}_{\sigma_{i_j}}(\mathbf{c}_{i_j})$, $j = 1, \dots, v$. В [10] показано, что система (4) имеет единственное решение тогда и только тогда, когда выполняется равенство (2) для множества $A = \{i_1, \dots, i_v\}$. В общем случае для произвольного $B \subseteq \underline{n}$, решая систему (4), можно найти

$$q^{\dim(\cap_{i \in B} \mathcal{L}_{\tau_i}(G))}$$

различных решений — возможных кандидатов на секрет $\mathbf{s}$. Таким образом, *структура доступа* $\mathcal{A}$ (набор правомочных коалиций участников) предлагаемой в настоящей работе СРС для заданного $\mathcal{T}$ определяется следующим образом:

$$\mathcal{A} = \{A \in 2^{\underline{n}} \setminus \emptyset : \text{для } A \text{ выполняется равенство (2)}\}, \quad (5)$$

где $2^{\underline{n}}$ — семейство всех подмножеств множества $\underline{n}$, $\emptyset$ — пустое множество.

Протоколом восстановления секрета является процедура нахождения правомочной коалицией $A = \{i_1, \dots, i_v\} (\in \mathcal{A})$ решения системы (4), т. е. вектора $\mathbf{s}$ (например, с помощью метода Гаусса).

Как видно из (3), особенностью предлагаемого в настоящей работе протокола разделения секрета является то, что для каждого участника вектор $\mathbf{a}_i$ выбирается случайно и независимо от других участников. С другой стороны, однозначное восстановление секрета по имеющимся долям зависит только от размерности подпространства $\cap_{j \in \{i_1, \dots, i_v\}} \mathcal{L}_{\tau_j}(G)$, но не зависит от того, какой именно вектор $\mathbf{a}_i$ использовался в (3). Поэтому возможна замена дилером любого i -го участника без изменения долей секрета у участников с номерами из множества $\underline{l} \setminus \{i\}$, либо же любой i -й участник может в любой момент модифицировать свою часть, прибавив к $\dot{\pi}_{\sigma_i}(\mathbf{c}_i)$ вектор $\dot{\pi}_{\sigma_i}(\mathbf{z}_i)$, где $\mathbf{z}_i$ выбирается из $C^\perp$ случайно и равномерно.

Обычно доли секрета имеют одинаковую длину для всех участников из $\mathcal{P}$. Тогда если ν — длина доли секрета для всех участников, то в определении (5) следует множество $2^{\underline{n}}$ заменить на $2^{\underline{n}, \nu}$ — множество всех подмножеств множества $\underline{n}$, каждое из которых (подмножество) имеет мощность ν . Интуитивно понятно, что чем больше ν (мощность множества σ_i , $i = 1, \dots, l$), тем меньше $|N_{\sigma_i}| = q^{\pi_{\tau_i}(G)}$, где $\tau_i = \underline{n} \setminus \sigma_i$, и тем коалиции меньшей мощности смогут восстановить секрет. Поэтому целесообразно найти значения ν , при которых возможна реализация СРС, а также значения, при которых предлагаемая в настоящей работе СРС не может быть реализована. С этой целью введем необходимые понятия. Пусть

$$T(n, \mu, l) = \{(\tau_1, \dots, \tau_l) : \forall i \in \underline{l} \ (\tau_i \subseteq \underline{n}) \wedge (|\tau_i| = \mu)\}$$

— множество, состоящее из всех возможных l -элементных семейств равно-мощных (мощности μ) подмножеств множества $\underline{n}$. Для линейного $[n, k, d]$ -кода C рассмотрим набор чисел (профиль):

$$I(C) = (l_0(C, 0), \dots, l_k(C, 0), l_0(C, 1), \dots, l_k(C, n)), \quad (6)$$

где для пары $(i, j) \in \underline{k}_0 \times \underline{n}_0$ величина $l_i(C, j)$ имеет вид

$$l_i(C, j) = \min \{l \in \mathbb{N} : \exists T \in T(n, j, l) \mid \dim(\cap_{\tau \in T} \mathcal{L}_\tau(G)) \leq i\}. \quad (7)$$

При этом будем считать, что при $j = 0$ размерность линейной оболочки, натянутой на пустое множество столбцов матрицы G , равна нулю, т. е. $l_i(C, 0) = 0$ для $i = 0, \dots, k$. Соответствующее числу $l = l_i(C, j)$ множество семейств $T(n, j, l)$ назовем *множеством минимальных семейств* и обозначим $T_i(n, j)$, $|T| = l_i(C, j)$ для всех T из $T_i(n, j)$. Минимальность здесь означает, что для заданной пары (i, j) множество $T_i(n, j)$ состоит только из семейств T мощности $l_i(C, j)$, удовлетворяющих условию $\dim(\cap_{\tau \in T} \mathcal{L}_\tau(G)) \leq i$. Будем писать $l_i(C, j) = \infty$, если для кода C не существует множества минимальных семейств для заданной пары (i, j) .

Лемма 1. Пусть G и Q — соответственно $(k \times r)$ - и $(k \times g)$ -матрицы над полем $\mathbb{F}$, $\mathcal{L}(G)$ и $\mathcal{L}(Q)$ — линейные подпространства пространства $\mathbb{F}^k$, порожденные столбцами этих матриц, $\dim(\mathcal{L}(G)) = r_0$, $r_0 \leq \min\{k, r\}$, $\dim(\mathcal{L}(Q)) = g_0$, $g_0 \leq \min\{k, g\}$, $P \in \text{GL}(k, \mathbb{F})$. Тогда

$$\dim(\mathcal{L}(G) \cap \mathcal{L}(Q)) = \dim(\mathcal{L}(PG) \cap \mathcal{L}(PQ)).$$

Доказательство. Рассмотрим матрицу $M = (G \ Q)$. Известно, что

$$\text{rank}(M) = \text{rank}(G) + \text{rank}(Q) - \dim(\mathcal{L}(G) \cap \mathcal{L}(Q)).$$

Отсюда

$$\dim(\mathcal{L}(G) \cap \mathcal{L}(Q)) = r_0 + g_0 - \text{rank}(M).$$

Утверждение леммы следует из того, что $\text{rank}(G) = \text{rank}(PG) = r_0$, $\text{rank}(Q) = \text{rank}(PQ) = g_0$, $\text{rank}(M) = \text{rank}(PM)$. $\square$

Если G и G' — разные порождающие матрицы $[n, k]$ -кода C , то найдется такая матрица $P \in \text{GL}(k, \mathbb{F})$, что $G' = PG$. Тогда из определения профиля (6) и леммы 1 следует, что профиль (6) является *характеристикой* кода C , так как не зависит от выбора порождающей матрицы кода. Поэтому вместо $\mathcal{L}_S(G)$ иногда будем использовать обозначение $\mathcal{L}_S(C)$. Кроме того, стоит отметить, что профиль инвариантен относительно перестановки столбцов порождающей матрицы, т. е. для комбинаторно-эквивалентных кодов профиль (6) будет одинаковым. Профиль (6) не изменится также, если столбцы порождающей матрицы умножить на ненулевые элементы поля $\mathbb{F}$. Отметим, что свойство инвариантности профиля может оказаться полезным, например при анализе стойкости кодовых криптосистем типа Мак-Элиса с использованием алгоритма расщепления носителя (support splitting algorithm) [11]. Учитывая потенциальные возможности применения профиля (6) в различных прикладных задачах, в следующем разделе профиль (6) исследуется не в рамках задачи построения и исследования СРС, а как характеристика $[n, k]$ -кода C .

3. Вычисление компонент профиля $l(C)$

Пусть $C_\tau = \{c \in C : \text{supp}(c) \subseteq \tau\}$ — укороченный код $[n, k]$ -кода C , $\tau \subseteq \underline{n}$. В дальнейшем нам понадобится следующее равенство (см. [12]):

$$\dim(\widehat{\pi}_\tau(C)) + \dim(C_\tau) = k. \quad (8)$$

Лемма 2. Пусть C — $[n, k, d]$ -код, $C^\perp$ — $[n, n - k, d^\perp]$ -код, ортогональный к коду C , $(j_1, j_2) \in \underline{n}_0 \times \underline{n}_0$, $j_1 > j_2$, $(i_1, i_2) \in \underline{k}_0 \times \underline{k}_0$, $i_1 > i_2$. Тогда:

- 1) $l_i(C, j_1) \geq l_i(C, j_2)$ для любого $i \leq j_2$,
- 2) $l_{i_1}(C, j) \leq l_{i_2}(C, j)$ для любого $j \geq i_1$,
- 3) $l_i(C, j) = 1$ для всех $(i, j) \in \underline{k} \times \underline{n}$ таких, что $i \geq j$,

$$4) \quad l_i(C, j) = \begin{cases} \left\lceil \frac{k-i}{k-j} \right\rceil & \text{при } j < d^\perp, i \leq j, k \neq d^\perp - 1, \\ \infty & \text{при } j > n - d, i < k, \\ 1 & \text{при } j > k, i = k, \end{cases}$$

где $\lceil a \rceil$ — ближайшее сверху целое к $a \in \mathbb{R}$.

Доказательство. Утверждения 1) и 2) вытекают непосредственно из определения (7). Для доказательства утверждения 3) достаточно заметить, что при $i \geq j$ всегда найдется хотя бы одно такое множество $\tau (\subseteq \underline{n})$, $|\tau| = j$, что $\dim(\mathcal{L}_\tau(G)) \leq i$. Докажем утверждение 4). Из теории линейных помехоустойчивых кодов известно, что при $j < d^\perp$ любые j столбцов порождающей матрицы G кода C линейно независимы. Отметим, что из неравенства Синглтона для кода $C^\perp$ получаем $k \geq d^\perp - 1$, поэтому из условия $k \neq d^\perp - 1$ следует, что $k > j$. Тогда минимальное семейство для заданных j и i можно построить следующим образом. На первом шаге выбирается любой набор τ_1 мощности j , на втором — такой набор τ_2 мощности j , что

$$\dim(\mathcal{L}_{\tau_1}(G) \cap \mathcal{L}_{\tau_2}(G)) = 2j - \min\{k, 2j\} =: d_{12}.$$

Если $d_{12} > i$ (т. е. $k < 2j$), то на третьем шаге выбирается такой набор τ_3 мощности j , что

$$\dim(\mathcal{L}_{\tau_1}(G) \cap \mathcal{L}_{\tau_2}(G) \cap \mathcal{L}_{\tau_3}(G)) = 2j - k + j - \min\{k, 3j - k\},$$

и так далее до тех пор, пока размерность пересечения станет не более i . Таким образом, $l_i(C, j)$ равно такому наименьшему неотрицательному целому числу l , при котором выполняется условие $lj - (l - 1)k \leq i$, откуда

$$l_i(C, j) = \left\lceil \frac{k - i}{k - j} \right\rceil.$$

При $j > n - d$ для любого τ , $|\tau| = j$, размерность проекции $\hat{\pi}_\tau(C)$ равна k , иначе в противном случае из (8) получили бы, что кодовое расстояние кода C меньше d . Таким образом, в этом случае $l_i(C, j) = \infty$ для $i < k$. Также $l_k(C, j) = 1$ для всех $j \geq k$, так как в порождающей матрице всегда найдется набор из k линейно независимых столбцов. $\square$

Напомним, что линейный $[n, k, d]$ -код называется кодом с максимальным достижимым расстоянием (МДР-кодом), если $n - k = d - 1$. Если для $[n, k, d]$ -кода C выполняется равенство $d + d^\perp = n$, где $d^\perp$ — кодовое расстояние $[n, n - k, d^\perp]$ -кода $C^\perp$, то код C называется почти-МДР-кодом [15].

Следствие 1. Пусть $[n, k, d]$ -код C является МДР-кодом или почти-МДР-кодом. Тогда

$$l_i(C, j) = \begin{cases} \left\lceil \frac{k-i}{k-j} \right\rceil & \text{при } j < k, i \leq j, \\ \infty & \text{при } j > k, i < k, \\ 1 & \text{при } j \geq k, i = k. \end{cases}$$

Для МДР-кода C также выполняется равенство $l_i(C, k) = \infty$ при $i < k$.

Доказательство. Если C — МДР-код, то $C^\perp$ — МДР-код, поэтому $k = d^\perp - 1$ и $n - d = k - 1$. Тогда доказываемые утверждения для МДР-кода следуют из утверждения 4) леммы 2. Доказательство утверждения для почти-МДР-кода C следует также из утверждения 4) леммы 2, так как для почти-МДР-кода C выполняются равенства $d = n - k$ и $d^\perp = k$ [15]. $\square$

Для $[n, k]$ -кода C и числа $i \in \underline{n}_0$ рассмотрим величины, впервые введенные в [12]:

$$\mathbf{k}_i(C) = \max_{\tau: |\tau|=i} \{\dim C_\tau\} \quad \text{и} \quad \tilde{\mathbf{k}}_i(C) = \min_{\tau: |\tau|=i} \{\dim \hat{\pi}_\tau(C)\}.$$

Из (8) вытекает, что $\mathbf{k}_i(C) + \tilde{\mathbf{k}}_{n-i}(C) = k$ для любого $i \in \underline{n}_0$.

Следствие 2. Пусть C — $[n, k, d]$ -код. Тогда $l_i(C, j) \geq \left\lceil \frac{k-i}{k-\mathbf{k}_j(C)} \right\rceil$ для $i \leq j$.

Доказательство. В случае $j < d^\perp$ утверждение совпадает с результатом из утверждения 4) леммы 2. При $j \geq d^\perp$ в общем случае наборы столбцов по j штук имеют разный ранг, отсюда получаем оценку снизу. $\square$

Заметим, что при $j \leq n - d$ для некоторых i в общем случае может выполняться равенство $l_i(C, j) = \infty$. Например, для бинарного $[4, 3, 1]$ -кода C с порождающей матрицей вида

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad (9)$$

только один набор из $j = 3$ столбцов имеет ранг 2, а остальные наборы ранга 3. Следовательно, $l_0(C, 3) = l_1(C, 3) = \infty$.

Лемма 3. Пусть C — $[n, k]$ -код. Тогда $l_i(C, j) \leq k$ для $j \leq k - 1$ и $i \leq j$.

Доказательство. Рассмотрим случай $j = k - 1$ и $i = 0$. Произвольную порождающую матрицу G кода C с помощью линейных операций над строками можно привести к псевдосистематическому виду $\tilde{G}$, т. е. к такому виду, когда найдется множество $\omega = \{w_1, \dots, w_k\} (\subseteq \underline{n})$ мощности k , что $\pi_\omega(\tilde{G})$ — единичная $(k \times k)$ -матрица [13]. При этом, с учетом леммы 1, линейные операции над строками порождающей матрицы не меняют профиль (6). Пусть $\bar{\omega} = \underline{n} \setminus \omega$, σ_s — носитель s -й строки матрицы $\tilde{G}$, $\sigma_s \subseteq \hat{\sigma}_s = \bar{\omega} \cup \{s\}$, $|\hat{\sigma}_s| = n - k + 1$, $\tau_s := \underline{n} \setminus \hat{\sigma}_s$, $s = 1, \dots, k$. Таким образом, для каждого $s = 1, \dots, k$ матрица $\hat{\pi}_{\tau_s}(\tilde{G})$ состоит из $k - 1$ столбцов единичной $(k \times k)$ -матрицы, поэтому $\dim(\mathcal{L}_{\tau_s}(C)) = k - 1$. По построению подпространства $\mathcal{L}_{\tau_s}(C)$ и $\mathcal{L}_{\tau_{s'}}(C)$ для $s \neq s'$ разные (как множества). Следовательно, $\dim(\cap_{s=1}^k \mathcal{L}_{\tau_s}(C)) = 0$. Отсюда $l_0(C, k - 1) \leq k$. Тогда для $j \leq k - 1$ и $i \leq j$ утверждение вытекает из пп. 1) и 2) леммы 2. $\square$

Из лемм 2 и 3 вытекает следующая теорема.

Теорема 1. Пусть C — $[n, k, d]$ -код, $C^\perp$ — $[n, n - k, d^\perp]$ -код, ортогональный к коду C , $i \in \mathbb{N}$, $i < k$. Тогда $l_i(C, j) \neq \infty$ при $0 \leq j \leq \max\{d^\perp - 1; k - 1\}$ и $l_i(C, j) = \infty$ при $j > n - d$.

Для $[n, k]$ -кода C и заданного числа $r (\in \{0, \dots, n\})$ рассмотрим множество векторов $C[r] = \{c \in C : w(c) \leq r\}$ и линейную оболочку $\mathcal{L}(C[r])$, натянутую на эти векторы, где $w(c) = |\text{supp}(c)|$. Пусть

$$W(C) = \{w_j = \dim(\mathcal{L}(C[j]))\}_{j=0}^n \quad (10)$$

и $\text{mgw}(C) = \min\{j : w_j = k\}$. Очевидно, что $C[q] \subseteq C[r]$ и $\mathcal{L}(C[q]) \subseteq \mathcal{L}(C[r])$ для $q < r$, поэтому $w_r \geq w_q$ и $w_j = k$ для $j \geq \text{mgw}(C)$. Несложно также проверить, что $w_j = 0$ для $j < d$.

Теорема 2. Пусть C — $[n, k]$ -код. Тогда $l_{k-w_j}(C, n - j) \leq w_j$.

Доказательство. Из определения (10) следует, что в коде C найдутся w_j линейно независимых векторов, вес которых не превышает j . Пусть $\sigma_1, \dots, \sigma_{w_j}$ — носители этих векторов для фиксированного j . Каждое из множеств σ_i , $i = 1, \dots, w_j$, дополним элементами из $\underline{n} \setminus \sigma_i$ до множеств $\hat{\sigma}_i$ мощности j , $\sigma_i \subseteq \hat{\sigma}_i$. Тогда для $\tau_i = \underline{n} \setminus \hat{\sigma}_i$, $|\tau_i| = n - j$, $i = 1, \dots, w_j$, имеем

$$\dim(\cap_{i=1}^{w_j} \mathcal{L}_{\tau_i}(C)) \leq k - w_j.$$

Отсюда и из определения (7) следует доказываемое утверждение. $\square$

Для $[n, k, d]$ -кода C последовательность чисел

$$d_i = \min_{0 \leq j \leq n} \{j : k_j(C) = i\}, \quad i = 1, \dots, k, \quad (11)$$

называется *иерархией обобщенных весов кода C* [14].

Следствие 3. Пусть C — $[n, k, d]$ -код, $(d_1, \dots, d_n)$ — его иерархия обобщенных весов. Тогда

- 1) $l_0(C, j) \leq k$ для $j \leq n - \text{mgw}(C)$,
- 2) если $\text{mgw}(C) < d_2$, то $l_{k-i}(C, n - \text{mgw}(C)) = i$.

Доказательство. Первое утверждение непосредственно следует из теоремы 2 и определения $\text{mgw}(C)$. Докажем второе утверждение. Для любого кодового вектора $\mathbf{c} \in C$ веса менее d_2 с носителем $\sigma = \text{supp}(\mathbf{c})$ имеем $\dim(C_\sigma) = 1$, так как минимальная мощность носителя кода размерности 2 равна d_2 (см. определение (11)). В частности, код C_σ состоит из векторов вида $a \cdot \mathbf{c}$, где $a \in \mathbb{F}$. Из (8) получаем, что если $\mathbf{c} \in C$ — любой вектор веса менее d_2 и $\tau = \underline{n} \setminus \text{supp}(\mathbf{c})$, то

$$\dim(\widehat{\pi}_\tau(C)) = \dim(\mathcal{L}_\tau(C)) = k - 1.$$

Для остальных τ мощности $n - \text{mgw}(C)$ имеем $\dim(\widehat{\pi}_\tau(C)) = k$. Из неравенства $d \leq \text{mgw}(C) < d_2$ и леммы 1 получаем, что в любой порождающей матрице кода G найдутся такие i наборов по $n - \text{mgw}(C)$ столбцов, что соответствующие линейные оболочки пересекаются только по подпространству размерности $k - i$. $\square$

Отметим, что характеристика $\text{mgw}(C)$ линейного кода C находит применение в некоторых прикладных задачах. Например, на основе этой величины может быть оценен минимальный объем выборки зашумленных кодовых слов, полученных из двоичного симметричного канала, достаточной для проверки гипотезы о принадлежности кодовых слов коду $C^\perp$ [16].

Под равновесным кодом далее понимается код, в котором веса всех ненулевых кодовых слов одинаковы.

Следствие 4. Пусть C — равновесный $[n, k, d]$ -код. Тогда

$$l_i(C, j) \begin{cases} \leq k - i & \text{при } j < n - d, \quad i \leq \min\{j, k - 1\}, \\ = k - i & \text{при } j = n - d, \quad i < k, \\ = \infty & \text{при } j > n - d, \quad i < k, \\ = 1 & \text{при } j \geq k, \quad i = k. \end{cases} \quad (12)$$

Доказательство. Так как $\dim(C_\sigma) = 0$ для любого $\sigma(\subseteq \underline{n})$ мощности менее d , то, с учетом (8), $l_i(C, j) = \infty$ для любого $j > n - d$ при $i < k$. Случай $i = k$ и $j \geq k$ следует из леммы 2. Пусть $j = n - d$, $i < k$. Так как код равновесный, то любая порождающая матрица этого кода состоит из векторов веса d . Зафиксируем некоторую порождающую матрицу $G = (\mathbf{g})_{i=1}^k$ равновесного кода C . Покажем, что для i ($0 \leq i < k$) любые разные $k - i$ строк $\mathbf{g}_{v_1}, \dots, \mathbf{g}_{v_{k-i}}$ матрицы G определяют некоторое семейство T из $T_i(n, n - d)$. Пусть $\sigma_s = \text{supp}(\mathbf{g}_{v_s})$, $\tau_s = \underline{n} \setminus \sigma_s$, $s = 1, \dots, k - i$, тогда $\dim(\cap_{s=1}^{k-i} \mathcal{L}_{\tau_s}(C)) = i$ и $T = \{\tau_1, \dots, \tau_{k-i}\}$. При этом для любого T' из $T(n, n - d, p)$ при $p < k - i$ неравенство $\dim(\cap_{\tau \in T'} \mathcal{L}_\tau(C)) \leq i$ не выполняется, так как для рассматриваемого кода C и любого τ мощности $n - d$ имеем: $\dim(\mathcal{L}_\tau(C)) = k$ или $\dim(\mathcal{L}_\tau(C)) = k - 1$ (минимальная размерность пересечения $p = k - (i + 1)$ и менее таких подпространств равна $i + 1$). Поэтому $T \in T_i(n, n - d)$. Случай $j < n - d$ и $i \leq \min\{j; k - 1\}$ вытекает из леммы 2. $\square$

Заметим, что для рассмотренных МДР-кодов, почти-МДР-кодов и равновесных кодов описания профиля (6), представленные в следствиях 1 и 4, получены благодаря тому, что для этих кодов выполняется равенство

$$\text{mgw}(C) = d, \quad (13)$$

где d — минимальное кодовое расстояние соответствующего кода C . Отметим, что равенство (13) означает, что код C порождается кодовыми словами минимального веса. Это свойство выполняется также для отдельных известных кодов. В частности, в [17] показано, что если $C = \mathcal{RM}_{\mathbb{F}_q}(\rho, m)$ — обобщенный код Рида–Маллера с минимальным кодовым расстоянием d , $q = p^t$, то в случаях, когда или $m = 1$, или $t = 1$, или $\rho < p$, или $\rho > (m - 1)(q - 1) + p^{t-1} - 2$, код порождается словами минимального веса. В [18, с. 185] доказано, что совершенные линейные коды (коды, для которых достигается граница Хэмминга или граница сферической упаковки) также порождаются кодовыми словами минимального веса. Отсюда следует, что для совершенного линейного $[n, k, d]$ -кода C также выполняется (13). Другим примером кодов, для которых выполняется (13), является семейство таких бинарных кодов $\mathcal{K}(r)$, $r \in \mathbb{N}$, $r \geq 2$, что код $K(r) (\in \mathcal{K}(r))$ порождается матрицей вида

$$G_r = \left(\begin{array}{c|c} G_{r-1} & I_r \\ \hline \mathbf{0}_{r-1} & \mathbf{1}_r \end{array} \right), \quad (14)$$

где I_r — единичная $(r \times r)$ -матрица, $\mathbf{0}_{r-1}$ — нулевая вектор-строка длины $(r - 1)r/2$, $\mathbf{1}_r$ — вектор-строка длины r , состоящая из единиц, $G_1 = (1 \ 1)^\top$.

Отметим, что в матрице G_r вида (14) в каждой строке r единиц, а в каждом столбце две единицы. Несложно показать, что $\dim(K(r)) = r - 1$ и минимальное кодовое расстояние d кода $K(r)$ равно r [19]. Отсюда, с учетом (14), получаем, что для любого кода $K(r)$ выполняется равенство (13).

Задача нахождения в коде C кодового слова заданного веса является NP-полной задачей [20], поэтому нахождение всех векторов кода с весом не более заданного (и, таким образом, построение набора (10)) представляется не менее трудной задачей. Поэтому в общем случае без знания структуры кода полное аналитическое описание профиля (6) затруднено. Однако для построения набора (10) в случае произвольного $[n, k]$ -кода C можно применить алгоритм поиска кодовых слов веса, не превышающего заданное число, разработанный в [21]. В частности, если представить порождающую матрицу кода C в псевдосистематическом виде, то для нахождения всех векторов веса не более j потребуется перебрать порядка $\sum_{s=1}^j C_k^s (q-1)^s$ кодовых слов.

Применяя результаты оценки статистических характеристик весовых спектров кодов из [22], можно получить статистическую оценку для профиля (6), когда $q = p$, где p — простое число. Пусть $L_{i,j}$ — случайная величина, принимающая значение $l_i(C, j)$, когда C выбирается случайно и равномерно среди $[n, k]$ -кодов над полем $\mathbb{F}_p$.

Лемма 4. Пусть C — $[n, k, d]$ -код, $A(x, y) = \sum_{s=0}^n A_s x^s y^{n-s}$ — нумератор весов C , $A_s = |\{\mathbf{c} \in C : w(\mathbf{c}) = s\}|$.

Тогда для $j = d, \dots, n$ и $s_j = \lceil \log_q (1 + \sum_{s=d}^j A_s) \rceil$

$$l_{k-s_j}(C, n-j) \leq s_j. \quad (15)$$

Доказательство. Так как $|C[j]| = 1 + \sum_{s=d}^j A_s$ для $j = d, \dots, n$, то размерность линейной оболочки $\mathcal{L}(C[j])$, натянутой на векторы множества $C[j]$, будет не менее $\lceil \log_q |C[j]| \rceil = s_j$. Тогда неравенство (15) следует из определения (10) и теоремы 2. $\square$

Лемма 5. Рассмотрим множество всех $[n, k]$ -кодов над полем $\mathbb{F}_p$, где p — простое число. Пусть $\mathbf{E} |C[j]|$ — математическое ожидание мощности множества $C[j]$, когда код C выбирается случайно и равномерно. Тогда

$$\mathbf{E} |C[j]| = \frac{p^k - 1}{p^n - 1} \sum_{s=0}^j C_n^s (p-1)^s. \quad (16)$$

Доказательство. Согласно [22, теорема 2, с. 32], если D — линейный $[n, m]$ -код, D^* — случайный $[n, m^*]$ -подкод кода D , $m^* < m$, $v_{\leq j}(D^*)$ и $v_{\leq j}(D)$ — количества векторов веса не более j соответственно в D^* и D , то

$$\mathbf{E}v_{\leq j}(D^*) = \frac{p^{m^*} - 1}{p^m - 1} v_{\leq j}(D).$$

Отсюда следует (16), если положить $m = n$, $m^* = k$, $D = \mathbb{F}_p^n$, $D^* = C$ и заметить, что $v_{\leq j}(\mathbb{F}_p^n) = \sum_{s=0}^j C_n^s (p-1)^s$. $\square$

Из леммы 4 и (16) получим следствие.

Следствие 5. Пусть k и n — натуральные числа, $k < n$, $j \in \underline{n}$,

$$S_j = \left\lceil \log_p \left(\frac{p^k - 1}{p^n - 1} \sum_{s=0}^j C_n^s (p-1)^s \right) \right\rceil.$$

Тогда $L_{k-S_j, n-j} \leq S_j$.

Если C — случайно и равномерно выбранный $[n, k]$ -код над $\mathbb{F}_p$, то для того, чтобы размерность пересечения δ линейных оболочек, натянутых на наборы столбцов порождающей матрицы, была не более $k - \delta$, достаточно, чтобы каждый набор состоял из $n - j$ столбцов, где $j \geq \min_{0 \leq \mu \leq n} \{\mu | S_\mu = \delta\}$. Поэтому k наборов дают в пересечении подпространство нулевой размерности, если

$$j \geq \min \left\{ \mu(\in \underline{n}) : \sum_{s=0}^{\mu} C_n^s (p-1)^s > \frac{p^{k-1}(p^n - 1)}{p^k - 1} \right\}. \quad (17)$$

Например, для бинарного $[8, 4, 4]$ -кода Рида–Маллера $C = \mathcal{RM}_{\mathbb{F}_2}(1, 3)$ из (13) получаем, что $\text{mgw}(C) = 4$. Отсюда $w_4 = \dim(C) = 4$, поэтому из теоремы 2 следует равенство

$$l_0(C, 4) \leq 4. \quad (18)$$

С другой стороны, из п. 4 леммы 2 следует, что $l_0(C, 3) = 4$, так как код C ортогонален сам себе. Так как $l_0(C, 3) \leq l_0(C, 4)$ (см. п.1 леммы 2), то $l_0(C, 4) = 4$. Заметим, что для этого кода оценка (15) совпадает с (18) при $j = 4$, так как нумератор весов этого кода имеет вид

$$A(x, y) = y^8 + 14x^4y^4 + x^8.$$

Оценка (17) для $[8, 4]$ -кодов над $\mathbb{F}_2$ показывает, что гарантированно найдутся 4 таких набора по $8 - j$ столбцов, что соответствующие линейные оболочки пересекаются по нуль-подпространству, если $j \geq 4$.

Рассмотрим другой пример. Пусть $C = K(4) - [10, 4, 4]$ -код, порождаемый строками матрицы вида (14) при $r = 4$. Выше было отмечено, что $\text{mgw}(C) = 4$, поэтому из следствия 3 получаем $l_0(C, 6) = 4$. Из (17) для $[10, 4]$ -кодов над $\mathbb{F}_2$ следует, что гарантированно найдутся 4 таких набора по $10 - j$ столбцов, что соответствующие линейные оболочки пересекаются по нуль-подпространству, если $j \geq 5$. В то же время для рассматриваемого кода $C = K(4)$ неравенство (15) дает оценку $l_0(C, 10 - j) \leq 4$ для $j \geq 6$, так как нумератор весов этого кода имеет вид $A(x, y) = y^{10} + 5x^4y^6 + 10x^6y^4$.

4. Некоторые реализации СРС типа схемы Блэкли

Пусть C — линейный $[n, k, d]$ -код над полем $\mathbb{F}_q$, $(d_1, \dots, d_n)$ — его иерархия обобщенных весов, $\mathcal{T} = \{\tau_1, \dots, \tau_k\} \in T_0(n, n - \text{mgw}(C))$, $|\tau_i| = n - \text{mgw}(C)$. Отметим, что семейство минимальных множеств $T_0(n, n - \text{mgw}(C))$ непустое в силу следствия 3. Так как $\text{mgw}(C) \geq d_1 = d$, то каждый участник по своей доле секрета сможет построить множество претендентов на секрет, и мощность этого множества будет меньше q^k , поэтому схема является несовершенной. Так как $|\mathcal{T}| = k$ и $\mathcal{T} \in T_0(n, n - \text{mgw}(C))$, то все k участников смогут восстановить секрет, решая систему вида (4).

Из следствия 3 получаем, что если $[n, k, d]$ -код C таков, что $\text{mgw}(C) = d$, то любые t ($t < k$) участников смогут уменьшить мощность множества претендентов на секрет до q^{k-t} . В этом случае построенная схема является несовершенной (k, k) -схемой разделения секрета; здесь и далее под (N, K) -схемой разделения секрета понимается такая схема, в которой любые K из N участников могут восстановить секрет. В частности, (k, k) -схема разделения секрета может быть построена с помощью любого $[n, k, d]$ -МДР-кода C , так как $\text{mgw}(C) = d$. Однако в этом случае схема не будет идеальной, так как $k \neq d$, и поэтому длина каждой доли секрета не будет равна длине секрета.

Лемма 6. Код $K(r)$, порожденный строками матрицы вида (14), для натурального $r (\geq 2)$ определяет идеальную (r, r) -схему разделения секрета.

Доказательство. Так как $\dim(K(r)) = r$, минимальное кодовое расстояние кода $K(r)$ равно r и $\text{mgw}(K(r)) = r$, то по коду $K(r)$ может быть построена (r, r) -схема разделения секрета, предложенная в настоящей работе. Множество $\mathcal{T}$ может быть построено по первым r строкам матрицы G_r : $\mathcal{T} = \{\tau_1, \dots, \tau_r\}$, где $\tau_i = \underline{n} \setminus \sigma_i$, σ_i — носитель i -й строки матрицы G_r . Так как $|\sigma_i| = r$ для всех $i = 1, \dots, r$, то каждый участник получает долю секрета длины r . Поэтому в силу равенства $\dim(K(r)) = r$ длина доли секрета равна длине секрета, и схема является идеальной. $\square$

Рассмотрим пример. Пусть $C = K(4)$ — $[10, 4, 4]$ -код, порождаемый строками матрицы вида (14) при $r = 4$:

$$G_4 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Так как $k = 4$, $\text{mgw}(C) = d = 4$ и $A_4 = 5$, то по строкам матрицы G можно построить все семейства для распределения долей секрета среди четырех участников. Именно, пусть

$$\sigma_1 = \{1, 2, 4, 7\}, \quad \sigma_2 = \{1, 3, 5, 8\}, \quad \sigma_3 = \{2, 3, 6, 9\},$$

$$\sigma_4 = \{4, 5, 6, 10\}, \quad \sigma_5 = \{7, 8, 9, 10\}.$$

Тогда по любым четырем элементам из множества $\mathcal{S} = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$ может быть построено соответствующее семейство $\mathcal{T}$ из $T_0(10, 6)$ для несовершенной $(4, 4)$ -схемы распределения секрета $s \in \mathbb{F}_2^4$ среди четырех участников. Заметим, что так как любые четыре строки матрицы G линейно независимы, то на основе кода C может быть построена несовершенная $(5, 4)$ -схема разделения секрета среди пяти участников, причем i -му участнику соответствует подмножество $\sigma_i \in \mathcal{S}$. В этом случае все подмножества мощности 4 семейства $\mathcal{S}$ образуют структуру доступа. Этот результат обобщается в следующей теореме.

Теорема 3. Код $K(r)$, порожденный строками матрицы вида (14), для любого натурального $r (\geq 2)$ определяет идеальную $(r+1, r)$ -схему разделения секрета.

Доказательство. Предъявим соответствующее множество $\mathcal{T}$. Пусть $\mathcal{S} = \{\sigma_1, \dots, \sigma_{r+1}\}$, где σ_i — носитель i -й строки матрицы G вида (14), $i \in \overline{r+1}$. Так как $\text{mgw}(K(r)) = r$ и любые r строк матрицы G линейно независимы, то система (4) будет иметь одно решение — секрет s — для любого подмножества мощности r множества $\mathcal{S}$. Поэтому $\mathcal{T} = \{\tau_1, \dots, \tau_{r+1}\}$, где $\tau_i = \underline{n} \setminus \sigma_i$, $i = 1, \dots, r+1$. Идеальность схемы следует из леммы 6. $\square$

В общем случае предложенная СРС типа схемы Блэкли не может быть совершенной в силу алгоритма восстановления секрета. Однако представляется, что эта система может найти применение в тех случаях, когда достаточно затруднить нарушителю или коалиции нарушителей получение секрета, например при защите нетекстовой информации.

Автор выражает благодарность рецензентам за конструктивную критику результатов и советы по их представлению, а также за полезные комментарии в части соотнесения результатов статьи с уже известными результатами из области схем распределения секрета и смежных областей. Автор также признателен редактору за тщательную вычитку текста, в результате чего удалось исправить ряд принципиальных опечаток и неточностей, которые существенно затрудняли понимание результатов работы.

Список литературы

- [1] Cramer R., Damgard I., Maurer U., “General secure multi-party computation from any linear secret-sharing scheme”. In: “*EUROCRYPT 2000*”, Lect. Notes Comput. Sci., **1807**, 2000, 316–334.
- [2] Chen H., Cramer R., Goldwasser S., Haan R., Vaikuntanathan V., “Secure computation from random error correcting codes”. In: “*EUROCRYPT 2007*”, Lect. Notes Comput. Sci., **4515**, 2007, 291–310.
- [3] Погорелов Б. А., Сачков В. Н., *Словарь криптографических терминов*, М.: МЦНМО, 2006, 91 с.
- [4] Shamir A., “How to share a secret”, *Comm. ACM*, **22**:11 (1979), 612–613.
- [5] Blakley G. R., “Safeguarding cryptographic keys”. In: “*AFIPS Conf. Proc.*”, **48**, 1979, 313–317..
- [6] Brickell E. F., “Some ideal secret sharing schemes”. In: “*EUROCRYPT’89*”, Lect. Notes Comput. Sci., **434**, 1989, 468–475.
- [7] Blakley G. R., Kabatianski G. A., “Linear algebra approach to secret sharing schemes”. In: “*Error Control, Cryptology, and Speech Compression*”, Lect. Notes Comput. Sci., **829**, 1994, 33–40..
- [8] Dijk M., “A linear construction of perfect secret sharing schemes”. In: “*EUROCRYPT’94*”, Lect. Notes Comput. Sci., **950**, 1994, 23–34.
- [9] Ozarov L. H., Wyner A. D., “Wire-tap channel II”, *Bell Labs Techn. J.*, **63**:10 (1984), 2135–2157..
- [10] Деундяк В. М., Косолапов Ю. В., “Об одном методе снятия неопределенности в канале с помехами в случае применения кодового зашумления”, *Изв. ЮФУ. Техн. науки* (2014), 197–208.
- [11] Sendrier N., “Finding the permutation between equivalent linear codes: the support splitting algorithm”, *IEEE Trans. Inf. Theory*, **46**:4 (2000), 1193–1203.
- [12] Forney G. D., “Dimension/length profiles and Trellis complexity of linear block codes”, *IEEE Trans. Inf. Theory*, **40**:6 (1994), 1741–1752.
- [13] Деундяк В. М., Маевский А. Э., Могилевская Н. С., *Методы помехоустойчивой защиты данных*, Ростов-н/Д: ЮФУ, 2014, 308 с.
- [14] Wei V. K., “Generalized Hamming weights for linear codes”, *IEEE Trans. Inf. Theory*, **37**:5 (1991), 1412–1418.
- [15] Dodunekov S. M., Landgev I. N., “On near-MDS codes”. In: “*Proc. IEEE Int. Symp. Inf. Theory*”, 1994, 427.
- [16] Chabot C., “Recognition of a code in a noisy environment”. In: “*Proc. IEEE Int. Symp. Inf. Theory*”, 2007, 2211–2215.
- [17] Ding P., Key J. D., “Minimum-weight codewords as generators of generalized Reed–Muller codes”, *IEEE Trans. Inf. Theory*, **46**:6 (2000), 2152–2157.

- [18] Blake I. F., Mullin R. C., *The Mathematical Theory of Coding*, N.Y.: Academic Press, 1975, 368 pp.
- [19] Косолапов Ю. В., “Верхняя граница иерархии весов регулярных слабоплотных кодов специального вида”, *Интегро-дифф. операторы и их прил. Межвуз. сб. науч. тр.*, № 8 (2008), 72–80.
- [20] Барг С., “Некоторые новые NP-полные задачи кодирования”, *Проблемы передачи информации*, **30**:3 (1994), 23–28.
- [21] Bouyukliev I., Bakoev V., “A method for efficiently computing the number of codewords of fixed weights in linear codes”, *Discr. Appl. Math.*, **156**:15 (2008), 2986–3004.
- [22] Зубков А. М., Круглов В. И., “Статистические характеристики весовых спектров случайных линейных кодов на $GF(p)$ ”, *Математические вопросы криптографии*, **5**:1 (2014), 27–38.