Моделирование и анализ информационных систем. Т. 26, № 2 (2019), с. 229–243
Modeling and Analysis of Information Systems. Vol. 26, No 2 (2019), pp. 229–243

DOI: 10.18255/1818-1015-2019-2-229-243

УДК 517.9

Система распределения ключей на дизайнах Адамара

Деундяк В. М., Таран А. А.

Поступила в редакцию 04 апреля 2019
После доработки 20 мая 2019
Принята к публикации 22 мая 2019

Аннотация. Изучается актуальная задача распределения ключей в сообществе для обеспечения безопасности переписки между ее участниками. Для решения этой задачи могут рассматриваться системы предварительного распределения ключей в сообществе, при этом каждый пользователь получает некоторую ключевую информацию, на основе которой он затем может независимо от других участников системы вычислить необходимые общие секретные ключи для тех конференций, в которые он входит. Такие системы предварительного распределения ключей могут быть основаны на разных базовых структурах, в частности, на помехоустойчивых кодах и комбинаторных дизайнах. Слабостью подобных систем является возможность проведения коалиционных атак, когда недобросовестные пользователи системы могут объединиться в коалицию и на основе всей имеющейся у них ключевой информации попытаться вычислить общие секретные ключи других участников сообщества. Однако системой гарантируется безопасность ключей в случае, если мощность коалиции злоумышленников не превышает некоторого значения, которое определяется конструкцией системы.

В работе рассматривается разработанная нами система распределения ключей, основанная на комбинаторных дизайнах, а именно на 3-дизайнах Адамара, гарантирующая безопасность переписки пользователей при наличии коалиции из не более чем двух злоумышленников. Для исследования стойкости системы к коалиционным атакам в случае превышения предусмотренного значения мощности коалиции вводятся новые понятия комбинаторной оболочки и комбинаторного ранга подмножества кода Адамара и изучаются некоторые комбинаторные свойства кодов Адамара. Для построенной системы распределения ключей вычисляется вероятность успешного проведения коалиционной атаки на произвольную конференцию в зависимости от мощности коалиции злоумышленников.

Ключевые слова: системы распределения ключей, комбинаторные дизайны, коалиционные атаки

Для цитирования: Деундяк В. М., Таран А. А., "Система распределения ключей на дизайнах Адамара", *Моделирование и анализ информационных систем*, **26**:2 (2019), 229–243.

Об авторах:
Деундяк Владимир Михайлович, orcid.org/0000-0001-8258-2419, канд. физ.-мат. наук, доцент,
Южный Федеральный Университет,
ул. Большая Садовая, 105/42, г. Ростов-на-Дону, 344006 Россия,
ФГНУ НИИ «Спецвузавтоматика»,
пер. Газетный, 51, г. Ростов-на-Дону, 344002, Россия, e-mail: vl.deundyak@gmail.com

Таран Алексей Александрович, orcid.org/0000-0002-1357-9360, аспирант,
Южный Федеральный Университет,
ул. Большая Садовая, 105/42, г. Ростов-на-Дону, 344006 Россия, e-mail: fraktal-at@yandex.ru

Введение

В многопользовательских системах передачи данных для того, чтобы обеспечить защиту переписки группы участников этой системы, используются криптографические алгоритмы, многие из которых требуют наличия у всех членов группы общего секретного ключа [1]. Для того, чтобы получить этот ключ, могут использоваться алгоритмы выработки общего секретного ключа [2], в которых члены группы обмениваются своими открытыми ключами и на их основе вычисляют общий секретный ключ, или системы распределения ключей [3], в которых участники получают общий секретный ключ, обмениваясь данными с неким доверенным сервером. Однако в некоторых случаях обмен данными с другими членами группы или с доверенным сервером может быть невозможен или непрактичен. В указанных случаях могут использоваться системы предварительного распределения ключей [4]. В таких системах каждый участник заранее получает ключевую информацию, на основе которой он может самостоятельно вычислить с помощью оговоренного алгоритма общий секретный ключ для любой группы, участником которой он является. Простейшим примером такой системы будет система, в которой каждый пользователь получит один и тот же общий секретный ключ для общения с любым другим участником системы. Однако такая система будет неустойчива к атакам – возможный злоумышленник внутри системы будет иметь такой же ключ, как и у всех остальных пользователей, и сможет получить доступ ко всем данным, передаваемым в системе. Другим примером является система, в которой каждый пользователь получит открытые ключи всех остальных пользователей в качестве своей предварительной ключевой информации. Такая система позволит пользователям вычислить необходимые общие ключи. Но с увеличением числа пользователей данной системы, а следовательно, и числа групп, которые могут организовывать конференции, будет расти и объем предварительной ключевой информации, которую потребуется хранить каждому пользователю.

Поэтому актуальной является разработка таких систем, которые, с одной стороны, позволяют уменьшить размер предварительно распределяемой информации, а с другой стороны, не позволяют даже нескольким злоумышленникам, объединившимся в коалицию, получить доступ к переписке других пользователей. Примерами таких систем являются полилинейные системы распределения ключей [5–7], а также системы предварительного распределения ключей, построенные на основе шаблонов распределения ключей [8]. В качестве основы для построения последних могут использоваться различные комбинаторные структуры, такие как ортогональные массивы и комбинаторные дизайны [9], как это было показано, например, в [10] и [11]. Подробный обзор различных подходов для построения таких систем можно найти в [12]. Системы данного типа гарантируют безопасность ключей, при условии, что размер коалиции злоумышленников не превышает некоторого значения, определяемого конструкцией системы. Однако в случае превышения этого значения коалиция злоумышленников может получить возможность вычислить часть общих секретных ключей для переписок других пользователей. Анализ таких коалиционных атак для полилинейных систем, построенных на кодах Хэмминга и Рида–Маллера второго порядка, проведен в работах [13, 14].

Целью настоящей работы является построение и исследование стойкости системы распределения ключей, основанной на комбинаторных 3-дизайнах Адамара. В разделе 1. представлена система, которая построена на основе шаблонов распределения ключей. Полученная система гарантирует безопасность переписки пользователей при наличии коалиции из не более чем двух злоумышленников. В разделе 3. для исследования стойкости системы вычисляется вероятность успешного проведения коалиционной атаки на общие секретные ключи конференций в зависимости от степени превышения мощности коалиции злоумышленников. Эти результаты получены на основе изучения комбинаторных свойств кода Адамара, которым посвящен раздел 2.

1. Конструкция системы распределения ключей на дизайнах Адамара

Система распределения ключей строится на основе шаблонов распределения ключей, предложенных в [8]. Эти шаблоны описаны в разделе 1.1. В разделе 1.2. содержатся необходимые сведения о дизайнах Адамара, а конструкция системы представлена в разделе 1.3.

1.1. Шаблоны распределения ключей

Предположим, что имеется сообщество из n пользователей, которым требуется возможность проведения конференций. Пусть $\mathcal{U}$ – множество идентификационных номеров, каждый из которых взаимнооднозначно соответствует пользователю системы, $|\mathcal{U}| = n$. Через $\mathcal{P}$ будем обозначать множество всех возможных конференций, каждая конференция $P \in \mathcal{P}$ является подмножеством $\mathcal{U}$ и содержит идентификационные номера всех участников конференции. Рассмотрим задачу предварительного распределения ключей пользователям из множества $\mathcal{U}$ для последующего вычисления ими общих секретных ключей для конференций из $\mathcal{P}$.

Предварительным распределением ключей занимается доверенный сервер. Для этого ему понадобится следующая конструкция.

Введем множество блоков $\mathcal{B} = \{B^{(1)}, \dots B^{(\beta)}\}$, каждый блок $B^{(i)} \in \mathcal{B}$ является подмножеством $\mathcal{U}$. Каждому блоку $B^{(i)}$ сервер ставит в соответствие ключ $k^{(i)}$ из множества ключей $\mathcal{K}$. После этого распределение ключей происходит следующим образом. Все пользователи системы знают множество идентификационных номеров $\mathcal{U}$ и множество блоков $\mathcal{B}$, которые являются публичной информацией. Каждый пользователь получает от сервера ключ $k^{(i)}$, если его идентификационный номер $u^{(j)}$ находится в соответствующем блоке $B^{(i)}$. Т.к. идентификационный номер $u^{(j)}$ может одновременно принадлежать нескольким блокам $B^{(i)}$, то в качестве секретной информации у каждого пользователя будет несколько ключей $k^{(i)} \in \mathcal{K}$.

Для того, чтобы участники конференции $P \in \mathcal{P}$ могли вычислить общий секретный ключ, необходимо, чтобы $\mathcal{B}_P = \{B^{(i)} \in \mathcal{B} | P \subseteq B^{(i)}\} \neq \oslash$, т.е. чтобы существовал как минимум один блок, содержащий в себе идентификационные номера всех участников конференции P. Далее введем множество $\mathcal{K}_P = \{k^{(i)} \in \mathcal{K} | B^{(i)} \in \mathcal{B}_P\}$ общих ключей участников конференции P. Отметим, что множество $\mathcal{K}_P$ непусто, т.к. непу-

сто множество $\mathcal{B}_P$. Тогда участники конференции могут вычислить на основе $\mathcal{K}_P$ общий секретный ключ конференции с помощью публичной функции f, действующей из множества всех подмножеств $\mathcal{K}$ в некоторое ключевое пространство $\mathfrak{K}$. Ключ k_P конференции P вычисляется как:

$$k_P = f(\mathcal{K}_P). \tag{1}$$

Функция f выбирается таким образом, чтобы обеспечить совершенную секретность общего ключа (см. [7], с. 287 и [10], с. 217). В частности, общий секретный ключ можно вычислить только при условии, если имеется все множество общих ключей конференции $\mathcal{K}_P$. Например, в качестве такой функции может использоваться побитовая сумма всех общих ключей.

В сообществе предполагается наличие злоумышленников, которые могут объединяться в коалиции и обмениваться своей секретной информацией с целью получить секретные ключи конференций, участниками которых они не являются. Обозначим множество возможных коалиций в системе через $\mathcal{F}$, где каждая коалиция $F \in \mathcal{F}$ является подмножеством $\mathcal{U}$. Для того, чтобы злоумышленники не могли напрямую вычислить по формуле (1) общие секретные ключи конференций, в которые они не входят, необходимо, чтобы выполнялось следующее условие:

$$\forall P \in \mathcal{P}, \forall F \in \mathcal{F}, \{B^{(i)} | P \subseteq B^{(i)} \ \wedge \ F \cap B^{(i)} = \oslash\} \neq \oslash, \tag{2}$$

то есть существует по крайней мере один ключ $k^{(j)}$, который известен всем участникам конференции P, но неизвестен ни одному из злоумышленников из коалиции F и, следовательно, коалиция F не может напрямую вычислить общий секретный ключ K_P по формуле (1).

При выполнении условия (2) $(\mathcal{U}, \mathcal{B})$ – называется шаблоном распределения ключей для $(\mathcal{P}, \mathcal{F})$ и обозначается $(\mathcal{P}, \mathcal{F})$-KDP ($(\mathcal{P}, \mathcal{F})$ Key Distribution Pattern). В случае, когда $\mathcal{P}$ – все подмножества $\mathcal{U}$ мощности t, а $\mathcal{F}$ – все подмножества $\mathcal{U}$ мощности не более чем w, $(\mathcal{P}, \mathcal{F})$-KDP обозначается как (t, w)-KDP.

Таким образом, шаблон (t, w)-KDP может быть использован для построения системы распределения ключей, которая позволяет организовывать защищенные конференции для групп из t участников системы и при этом гарантирует безопасность всех общих секретных ключей, при условии наличия внутри системы коалиции злоумышленников размера не более чем w.

1.2. Дизайны Адамара

В качестве шаблонов распределения ключей ниже применяются комбинаторные дизайны Адамара, которые строятся с помощью симметричных матриц $2^a \times 2^a$ Адамара-Сильвестра [15]:

$$H_a = \underbrace{H_1 \otimes \ldots \otimes H_1}_{a}, \ H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Матрицу Адамара далее будем записывать в двоичном виде, т.е. заменим $1, -1$ на элементы $0, 1$ из поля $\mathbb{F}_2$ соответственно, и будем использовать прежнее обозначение H_a. Множество всех столбцов или, что тоже самое, строк матрицы H_a будем

обозначать $\mathcal{A}_a$. Множество $\mathcal{A}_a$ вложено в $\mathbb{F}_2^n$ и $|\mathcal{A}_a| = n$, где $n = 2^a$. Это множество образует $[n, a, n/2]$-код Адамара, при этом строки с номерами $2^{j-1} + 1, j = 1, \ldots, a$ образуют одну из кодовых матриц, порождающих этот код, и являются базисом в $\mathcal{A}_a$. Например,

$$H_3 = \left(\begin{array}{cccccccc} 0&0&0&0&0&0&0&0\\ 0&1&0&1&0&1&0&1\\ \hline 0&0&1&1&0&0&1&1\\ \hline 0&1&1&0&0&1&1&0\\ 0&0&0&0&1&1&1&1\\ \hline 0&1&0&1&1&0&1&0\\ 0&0&1&1&1&1&0&0\\ 0&1&1&0&1&0&0&1 \end{array}\right),$$

где подчеркнутые строки являются базисом, порождающим все остальные строки матрицы.

Напомним, что ν-(n, k, λ)-дизайном называется пара $\{\mathcal{U}, \mathcal{B}\}$, где $\mathcal{U}$ – множество из $|\mathcal{U}| = n$ элементов (точек), а $\mathcal{B} = \{B^{(1)}, \ldots, B^{(\beta)}\}$ – множество подмножеств $\mathcal{U}$, мощность каждого $|B^{(j)}| = k$, для которой выполняется условие, что любые ν элемента из $\mathcal{U}$ содержатся ровно в λ блоках из $\mathcal{B}$ [9]. В теореме Стинсона в [10], с. 223, доказано, что $(t+1)$-(n, k, λ)-дизайн является (t, w)-KDP, при

$$w < \frac{n-t}{k-t}. \tag{3}$$

По матрице Адамара H_a можно построить 3-$(2^a, 2^{a-1}, 2^{a-2} - 1)$-дизайн следующим образом: в качестве $\mathcal{U}$ берется множество номеров столбцов матрицы, а блок $B^{(2(i-1)-1+\epsilon)}$, где $i \in \{2, \ldots, 2^a\}$, $\epsilon \in \{0, 1\}$, содержит номера тех столбцов, у которых в i-той строке стоит значение ϵ (см. [9], с. 116). В этом случае из параметров дизайна и условия (3) вытекает, что $w \leq 2$. Таким образом построенный дизайн Адамара является $(2, w)$-KDP, т.е. может использоваться для построения системы для конференций с двумя участниками, гарантируя безопасность общих секретных ключей при наличии коалиции злоумышленников из не более чем двух пользователей системы.

1.3. Построение системы

Предположим, что сообществу из $n = 2^a, a > 2$ пользователей требуется система для обеспечения безопасности переписки между любой парой пользователей.

Для построения этой системы сервер генерирует матрицу Адамара–Сильвестра H_a. Каждый столбец соответствует пользователю системы. По матрице Адамара в соответствии с разделом 1.2. определяется 3-$(n, n/2, n/4 - 1)$ дизайн Адамара. Для каждого блока $B^{(2(i-1)-1+\epsilon)}$, $i \in \{2, \ldots, n\}$, $\epsilon \in \{0, 1\}$, сервер генерирует секретный ключ $k^{(2(i-1)-1+\epsilon)}$, всего $2(n-1)$ блоков и ключей. Ключи распределяются следующим образом. Пользователь j получает ключ $k^{(2(i-1)-1+\epsilon)}$, если $j \in B^{(2(i-1)-1+\epsilon)}$. Так как по свойствам дизайнов этот дизайн также является 2-$(n, n/2, n/2 - 1)$ и 1-$(n, n/2, n-1)$ дизайном, то каждый пользователь получает $n-1$ секретный ключ, по одному из каждой пары $\{k^{(2(i-1)-1)}, k^{(2(i-1))}\}$, $i \in \{2, \ldots, n\}$, а у каждой пары пользователей имеется $n/2 - 1$ общих ключей. Блоки $B^{(2(i-1)-1+\epsilon)}$ являются открытой

информацией, с их помощью пользователи могут определить, какие у них общие ключи с другими участниками системы. На основе этих общих ключей пользователи могут вычислить общий секретный ключ для обеспечения безопасности их переписки при помощи заранее оговоренного алгоритма.

Находящиеся в системе пользователи-злоумышленники могут объединяться в коалиции и, собрав имеющиеся у них секретные ключи, могут попытаться получить все общие ключи других пользователей системы. В этом объединенном множестве ключей могут оказаться все общие ключи некоторой пары пользователей, не входящих в коалицию. В этом случае злоумышленники смогут вычислить их общий секретный ключ и будут иметь возможность читать переписку этих двух пользователей. По теореме Стинсона (3) построенная выше система является $(2, 2)$-системой, то есть гарантирует безопасность переписки пары пользователей при наличии в системе коалиции из не более чем двух злоумышленников.

Для того чтобы иметь возможность прочитать переписку двух конкретных пользователей, злоумышленникам необходимо получить все $n/2 - 1$ их общих ключей. В случае превышения предусмотренной мощности коалиции может получиться так, что коалиция получит все общие ключи двух пользователей и сможет вычислить общий секретный ключ для их переписки. Следующая теорема показывает, что если коалиции удается получить все общие ключи для переписки двух пользователей, то фактически она получает и все секретные ключи по крайней мере одного пользователя.

Теорема 1. *Для того, чтобы была возможна атака на общий ключ переписки двух участников, необходимо и достаточно, чтобы коалиция злоумышленников имела все ключи по крайней мере одного участника переписки.*

Доказательство. Достаточность. Если у коалиции злоумышленников имеются все ключи одного из участников конференции, то у коалиции, очевидно, есть и все общие ключи для любой переписки с его участием.

Необходимость. Предположим противное: коалиция злоумышленников получила все общие ключи некоторой переписки двух пользователей, но при этом у нее нет полного набора ключей ни одного из участников. Это значит, что существует номер i такой, что у первого участника переписки имеется ключ $k^{(2(i-1)-1+\epsilon_i)}$, а у каждого участника коалиции – другой ключ $k^{(2(i-1)-\epsilon_i)}$, и существует номер j такой, что у второго участника переписки имеется ключ $k^{(2(j-1)-1+\epsilon_j)}$, а у каждого участника коалиции – другой ключ $k^{(2(j-1)-\epsilon_j)}$. При этом если у первого участника переписки есть ключ $k^{(2(i-1)-1+\epsilon_i)}$, то у второго должен быть ключ $k^{(2(i-1)-\epsilon_i)}$: если бы у второго также был ключ $k^{(2(i-1)-1+\epsilon_i)}$, то это бы значило, что i-тый ключ у них общий, а т.к. по условию теоремы коалиция получила все общие ключи злоумышленников, то должна была получить и этот.

Покажем теперь, что i и j – различны. Предположим, что $i = j$. Как было показано ранее, i-тый ключ не является общим для участников переписки, т.е. у одного из участников будет ключ $k^{(2(i-1)-1+\epsilon)}$, а у другого $k^{(2(i-1)-\epsilon)}$. Но т.к. каждый пользователь системы получает один из каждой пары ключей, то не может быть, чтобы коалиция не получила ни одного ключа из этой пары. Следовательно $i \neq j$.

Рассмотрим теперь подматрицу матрицы Адамара, состоящую из строк i и j и

столбцов, соответствующих участникам переписки и коалиции злоумышленников. Строка i может быть записана одним из двух следующих вариантов:

$$\begin{array}{ccc|cc} 0 & \cdots & 0 & 1 & 0 \\ 1 & \cdots & 1 & 0 & 1 \end{array},$$

а строки j:

$$\begin{array}{ccc|cc} 0 & \cdots & 0 & 0 & 1 \\ 1 & \cdots & 1 & 1 & 0 \end{array}.$$

Возьмем любой из возможных вариантов строки i и прибавим к ней любой из вариантов строки j. В результате получится одна из следующих строк:

$$\begin{array}{ccc|cc} 0 & \cdots & 0 & 1 & 1 \\ 1 & \cdots & 1 & 0 & 0 \end{array}.$$

Так как строки матрицы Адамара состоят из всех слов кода Адамара, то любая сумма строк также является словом кода и строкой матрицы. Таким образом, мы получаем строку, в которой во всех позициях соответствующих участникам коалиции 0 (1), а в позициях, соответствующих участникам переписки – 1 (0). Это означает, что злоумышленники не получили общий ключ участников переписки, соответствующей этой строке, что противоречит условию. Следовательно, предположение, что коалиция получила все общие ключи участников переписки, но при этом не получила все ключи ни одного из них – неверно.

□

Эта теорема позволяет перейти от рассмотрения коалиционной атаки на все возможные переписки к рассмотрению атак на ключи других пользователей системы.

Так как по теореме 1 атака на ключ какой-то конкретной переписки эквивалентна атаке на все ключи одного из её участников, то можно ограничиться рассмотрением только атак на ключи пользователя. Отметим, что коалиция получает все ключи пользователя, когда она может составить вектор-столбец матрицы Адамара, соответствующий этому пользователю, из своих идентификационных столбцов. Подробнее это рассматривается в модели коалиционных атак (раздел 3.) на основе изучения комбинаторных свойств кода Адамара, которым посвящен раздел 2.

2. Комбинаторные свойства столбцов матриц Адамара

Будем обозначать через b_i значение i-той координаты произвольного вектора $b \in \mathbb{F}_2^n$. Для произвольного множества $B \subset \mathbb{F}_2^n$ обозначим $B_i := \{b_i | b \in B\} \subset \mathbb{F}_2$, а для произвольного непустого множества $D \subset \mathbb{F}_2$ обозначим $I_D(B) := \{i \in \{1, \ldots, n\} | B_i = D\}$. Таким образом, для любого множества B множество номеров $\{1, \ldots, n\}$ разбивается на три непересекающихся подмножества $I_{\{0\}}(B)$, $I_{\{1\}}(B)$ и $I_{\{0,1\}}(B)$.

Будем говорить, что вектор $a \in \mathbb{F}_2^n$ комбинаторно-зависим от множества $B \subset \mathbb{F}_2^n$, если для любого $i \in \{1, \ldots, n\}$ выполняется: $a_i \in B_i$. В противном случае будем

говорить, что a не является комбинаторно-зависимым от B. Если a комбинаторно-зависим от B, т.е.

$$a \in \mathrm{desc}(B) := \{(a_1, \ldots, a_n) : a_i \in B_i\},$$

то его называют потомком множества B [16]. Будем говорить, что вектор a строго комбинаторно-зависим от B, если он комбинаторно-зависим от B, но независим от любого собственного подмножества B.

Если $B \subset A \subset \mathbb{F}_2^n$, то комбинаторной оболочкой множества B во множестве A будем называть множество $< B >_A := \mathrm{desc}(B) \cap A$. Нетрудно доказать, что

$$\mathrm{desc}(\mathrm{desc}(B)) = \mathrm{desc}(B),\ << B >_A >_A = < B >_A,\ < A >_A = A. \tag{4}$$

Множество векторов будем называть комбинаторно-независимым, если любой его элемент комбинаторно-независим от множества, состоящего из остальных векторов. Комбинаторно-независимое подмножество множества B будем называть максимальным, если не существует другого комбинаторно-независимого подмножества, в которое это множество вложено.

Следующая лемма вытекает непосредственно из определений.

Лемма 1. *Пусть $\Lambda \subset A \subset \mathbb{F}_2^n$ и $\Lambda' \subset A \subset \mathbb{F}_2^n$. Для того, чтобы $< \Lambda >_A = < \Lambda' >_A$ необходимо и достаточно, чтобы $I_D(\Lambda) = I_D(\Lambda')$ для любого непустого $D \subset \mathbb{F}_2$.*

Лемма 2. *Пусть A – линейное пространство над полем $\mathbb{F}_2$, $\Lambda \subset A$. $< \Lambda >_A$ является подпространством A тогда и только тогда, когда $I_{\{1\}}(\Lambda) = \oslash$.*

Доказательство. Пусть $\Theta = \{\theta \in F_2^n | \theta_i = 0, i \in I_{\{0\}}(\Lambda)\}$. Достаточность является следствием следующего равенства: $< \Lambda >_A = A \cap \Theta$. Так как любой вектор $c \in < \Lambda >_A$ является потомком векторов из Λ, то $c_i = 0$ для $i \in I_{\{0\}}(\Lambda)$, и, следовательно, $c \in \Theta$. С другой стороны, любой вектор из $d \in A \cap \Theta$ будет иметь $d_i = 0$ для $i \in I_{\{0\}}(\Lambda)$ и $d_j = 0$ или $d_j = 1$ для $j \in I_{\{0,1\}}(\Lambda)$, и, следовательно, является потомком Λ и входит в $< \Lambda >_A$. Таким образом, $< \Lambda >_A = A \cap \Theta$ и является линейным подпространством A.

Необходимость докажем методом от противного: предположим, что комбинаторная оболочка $< \Lambda >_A$ является линейным подпространством A и при этом $I_{\{1\}}(\Lambda) \neq \oslash$. Это значит, что есть такая позиция i, на которой во всех векторах из Λ стоит единица, а значит и во всех векторах из $< \Lambda >_A$. Отсюда получаем, что в $< \Lambda >_A$ нет нулевого вектора, что противоречит предположению, что $< \Lambda >_A$ является линейным подпространством. □

Теперь рассмотрим свойства комбинаторной зависимости на множестве столбцов $\mathcal{A}_a$.

Замечание. Зафиксируем порождающую матрицу $G^{(1)}$ кода Адамара и рассмотрим другую порождающую матрицу $G^{(2)}$ этого же кода. Тогда найдется такая обратимая матрица S, что $SG^{(1)} = G^{(2)}$. Нетрудно показать, что в этом случае найдется такая перестановочная матрица P, что $SG^{(1)} = G^{(1)}P$, т.е. $G^{(2)} = G^{(1)}P$ (см., например, [15], с. 228).

Лемма 3. *Мощность произвольного максимального комбинаторно-независимого подмножества в $\mathcal{A}_a$ больше a.*

Доказательство. Для того, чтобы комбинаторно-независимое множество было максимальным необходимо, чтобы его комбинаторная оболочка была равна $\mathcal{A}_a$, в противном случае можно взять вектор, который не попал в комбинаторную оболочку и получить другое комбинаторно-независимое множество, в которое вложено исходное, что противоречит определению максимального комбинаторно-независимого множества. Таким образом, $< \Lambda >_{\mathcal{A}_a} = \mathcal{A}_a$ и, следовательно, $< \Lambda >_{\mathcal{A}_a} = < \mathcal{A}_a >_{\mathcal{A}_a}$. По лемме 1 для любого непустого $D \subset \mathbb{F}_2^n$ имеет место равенство $I_D(\Lambda) = I_D(\mathcal{A}_a)$. Отсюда вытекает:

$$I_{\{0,1\}}(\Lambda) = \{2, \ldots, n\}, I_{\{0\}}(\Lambda) = \{1\}, I_{\{1\}}(\Lambda) = \oslash. \tag{5}$$

Рассмотрим все подмножества $\mathcal{A}_a$ мощности a и покажем, что ни одно из них не является максимальным комбинаторно-независимым подмножеством $\mathcal{A}_a$.

Сначала рассмотрим базис B пространства $\mathcal{A}_a$, описанный в разделе 1.2. Тогда

$$I_{\{0,1\}}(B) = \{2, \ldots, n-1\}, I_{\{0\}}(B) = \{1\}, I_{\{1\}}(B) = \{n\}.$$

В силу леммы 1 и равенств (5) $< B >_{\mathcal{A}_a} \neq < \Lambda >_{\mathcal{A}_a} = \mathcal{A}_a$, т.е. множество B не является максимальным комбинаторно-независимым подмножеством $\mathcal{A}_a$.

От базиса B можно перейти к любому другому базису B' с помощью последовательности элементарных преобразований, т.е. умножением слева на некоторую обратимую матрицу.

В силу замечания в результате перехода от B к B' фактически переставляются координаты векторов из B. После перестановки столбцов для любого непустого $D \subset \mathbb{F}_2^n$ получим $|I_D(B)| = |I_D(B')|$, а значит $I_{\{1\}}(B') \neq I_{\{1\}}(\Lambda) = \oslash$ и, по лемме 1, $< B' >_{\mathcal{A}_a} \neq \mathcal{A}_a$. Следовательно, никакой базис в $\mathcal{A}_a$ не является максимальным комбинаторно-независимым множеством.

Рассмотрим множество $C \subset \mathcal{A}_a$ и предположим, что $|C| = a$ и $\mathrm{rank}(C) = k < a$, т.е. в C имеется подмножество C' из k линейно независимых векторов, а остальные $a - k$ векторов являются их линейными комбинациями. Тогда $|I_{\{0\}}(C)| = 2^{a-k}$, т.к. имеется 2^{a-k} координат, на которых у векторов из C', а значит и у их линейных комбинаций, стоят только нули. Так как $k < a$, то $|I_{\{0\}}(C)| > 1$, и, следовательно, $< C >_{\mathcal{A}_a} \neq < \Lambda >_{\mathcal{A}_a} = \mathcal{A}_a$, а значит C не является максимальным комбинаторно-независимым подмножеством $\mathcal{A}_a$.

Таким образом, никакое подмножество $\mathcal{A}_a$ мощности a не является максимальным комбинаторно-независимым подмножеством. □

Лемма 4. *Во множестве столбцов $\mathcal{A}_a$ аддитивной матрицы Адамара рассмотрим множество $\Lambda = \{\lambda^{(i)}\}_{i=1}^{w}$.*

1. *Если Λ' – максимальное комбинаторно-независимое подмножество Λ, то $< \Lambda >_{\mathcal{A}_a} = < \Lambda' >_{\mathcal{A}_a}$.*
2. *$|< \Lambda >_{\mathcal{A}_a}| = 2^{\nu}$ для некоторого ν.*
3. *Пусть $w \leq a + 1$. Если Λ – комбинаторно-независимое множество, то $|< \Lambda >_{\mathcal{A}_a}| = 2^{w-1}$.*
4. *Если Λ' и Λ'' – различные максимальные комбинаторно-независимые подмножества Λ, то $|\Lambda'| = |\Lambda''|$.*

Доказательство.

1. Предположим, что это не так. Тогда $< \Lambda >_{\mathcal{A}_a} \supsetneq < \Lambda' >_{\mathcal{A}_a}$. Следовательно в $< \Lambda >_{\mathcal{A}_a}$ существует элемент a, который комбинаторно зависит от Λ, но не зависит от Λ', а значит существует такая позиция i, что $a_i \in \Lambda_i = \{\lambda_i | \lambda \in \Lambda\}$, но $a_i \notin \Lambda'_i = \{\lambda'_i | \lambda' \in \Lambda'\}$. Из максимальности Λ' вытекает, что все элементы из Λ комбинаторно-зависимы от Λ', и поэтому $\Lambda_i = \Lambda'_i$ для любого i. Из полученного противоречия вытекает $< \Lambda >_{\mathcal{A}_a} = < \Lambda' >_{\mathcal{A}_a}$.

2. Пусть $\Lambda' = \{\lambda'^{(i)} = \lambda^{(i)} - \lambda^{(1)}\}_{i=1}^{w}$. Тогда

$$I_{\{0,1\}}(\Lambda') = I_{\{0,1\}}(\Lambda),\ I_{\{0\}}(\Lambda') = I_{\{0\}}(\Lambda) \cup I_{\{1\}}(\Lambda),\ I_{\{1\}}(\Lambda') = \oslash. \tag{6}$$

   При этом $| < \Lambda >_{\mathcal{A}_a} | = | < \Lambda' >_{\mathcal{A}_a} |$. Действительно, $< \Lambda >_{\mathcal{A}_a}$ состоит из всех столбцов множества $\mathcal{A}_a$, у которых одновременно стоят нули в позициях $I_{\{0\}}(\Lambda)$ и единицы в позициях $I_{\{1\}}(\Lambda)$. С другой стороны, $< \Lambda' >_{\mathcal{A}_a}$ состоит из всех столбцов $\mathcal{A}_a$, у которых стоят нули в позициях $I_{\{0\}}(\Lambda) \cup I_{\{1\}}(\Lambda)$. Векторы из множества $< \Lambda' >_{\mathcal{A}_a}$ могут быть получены из множества векторов $< \Lambda >_{\mathcal{A}_a}$ вычитанием вектора $\lambda^{(i)}$. Таким образом, $| < \Lambda >_{\mathcal{A}_a} | = | < \Lambda' >_{\mathcal{A}_a} |$.

   В силу (6) по лемме 2 $< \Lambda' >_{\mathcal{A}_a}$ является линейным подпространством в $\mathcal{A}_a$, следовательно, мощность $< \Lambda >_{\mathcal{A}_a}$ равна степени двойки.

3. Докажем теперь, что $|< \Lambda >_{\mathcal{A}_a}| = 2^{w-1}$.

   При $w = 1$ утверждение верно: комбинаторная оболочка одноэлементного множества состоит из этого одного элемента, $2^{w-1} = 1$.

   Пусть $w > 1$. Рассмотрим множество $\Lambda' = \Lambda \backslash \{b\}$, где $b = \lambda^{(i)}$ для некоторого i. Множество Λ' очевидно комбинаторно-независимо, и в силу утверждения 2 $| < \Lambda' >_{\mathcal{A}_a} | = 2^{\nu'}$ для некоторого ν'. При этом элемент $b \in < \Lambda >_{\mathcal{A}_a}$, но $b \notin < \Lambda' >_{\mathcal{A}_a}$, т.к. множество Λ комбинаторно-независимо. Получаем, что

$$| < \Lambda >_{\mathcal{A}_a} | = 2^{\nu} > | < \Lambda' >_{\mathcal{A}_a} | = 2^{\nu'}, \tag{7}$$

   и, следовательно, $\nu > \nu'$.

   С другой стороны $< \Lambda >_{\mathcal{A}_a} \subseteq \mathcal{A}_a$, т.е. $|< \Lambda >_{\mathcal{A}_a}| \leq |\mathcal{A}_a| = n = 2^a$. При этом в силу (4) и утверждения 1 равенство достигается в случае, когда Λ является максимальным комбинаторно-независимым подмножеством $\mathcal{A}_a$.

   Предположим для начала, что $w \leq a + 1$. Построим из множества Λ цепочку множеств, $\{\Lambda^{(i)}\}_{i=1}^{a+1}$ по следующему правилу:

$$\Lambda^{(i)} = \begin{cases} \Lambda, & i = w \\ \Lambda^{(i+1)} \backslash \{b\}, & i < w, b \in \Lambda^{(i+1)} \\ \Lambda^{(i-1)} \cup \{c\}, & i > w, c \in \mathcal{A}_a \backslash < \Lambda^{(i-1)} >_{\mathcal{A}_a} \end{cases}.$$

   Для i от 0 до w такая цепочка, очевидно, может быть построена, а возможность построения цепочки для значений от $w + 1$ до $a + 1$ вытекает из леммы 3. Отметим, что $|\Lambda^{(i)}| = i$ и $\Lambda^{(i)} \subset \Lambda^{(i+1)}$.

Рассмотрим мощности комбинаторных оболочек множеств $\Lambda^{(i)}$:

$$1 = 2^0 = |< \Lambda^{(1)} >_{\mathcal{A}_a}| < |< \Lambda^{(2)} >_{\mathcal{A}_a}| < \cdots < |< \Lambda^{(a+1)} >_{\mathcal{A}_a}| \leq 2^a.$$

Согласно утверждению 2 мощность каждого из $< \Lambda^{(i)} >_{\mathcal{A}_a}$ равна степени двойки и $|< \Lambda^{(i)} >_{\mathcal{A}_a}| < |< \Lambda^{(i+1)} >_{\mathcal{A}_a}|$. Отсюда вытекает, что $|< \Lambda^{(i)} >_{\mathcal{A}_a}| = 2^{i-1}$, и для $i = w$ получаем доказываемое утверждение.

Покажем теперь, что случай $w > a + 1$ – невозможен. Построим аналогичную цепочку $\{\Lambda^{(i)}\}_{i=1}^{w}$

$$\Lambda^{(i)} = \begin{cases} \Lambda, & i = w \\ \Lambda^{(i+1)} \backslash \{b\}, & i < w, b \in \Lambda^{(i+1)} \end{cases}$$

и рассмотрим неравенства

$$1 = 2^0 = |< \Lambda^{(1)} >_{\mathcal{A}_a}| < |< \Lambda^{(2)} >_{\mathcal{A}_a}| < \cdots < |< \Lambda^{(w)} >_{\mathcal{A}_a}| \leq 2^a.$$

Здесь мы имеем $w > a + 1$ множеств, мощности которых различаются и равны степеням двойки, но только $a + 1$ степеней от 0 до a, отсюда получаем противоречие.

4. Для доказательства последнего утверждения предположим противное. Из утверждения 3 вытекает, что если Λ' и Λ'' имеют разные мощности, то и мощности их комбинаторных оболочек будут различными. Но из утверждения 1 получаем, что их комбинаторные оболочки должны быть равны комбинаторной оболочке множества Λ, т.е. иметь одинаковую мощность. Противоречие.

□

Лемма 4 позволяет ввести определение комбинаторного ранга $\mathrm{rank}_{\mathrm{comb}}(\Lambda)$ множества Λ как мощность любого его максимального комбинаторно-независимого подмножества и получить следующую теорему.

Теорема 2. *Рассмотрим множество столбцов аддитивной матрицы Адамара $\mathcal{A}_a$ и рассмотрим в нем произвольное множество Λ. Мощность комбинаторной оболочки Λ в множестве $\mathcal{A}_a$*

$$|< \Lambda >_{\mathcal{A}_a}| = 2^{\mathrm{rank}_{\mathrm{comb}}(\Lambda)-1}.$$

3. Вероятности успешного проведения коалиционных атак в системе распределения ключей в случае превышения предусмотренной мощности коалиции

Для оценки стойкости, построенной в разделе 1., системы распределения ключей вычислим вероятности успешного проведения коалиционной атаки в зависимости от мощности коалиции злоумышленников.

Будем считать, что коалиция злоумышленников формируется заранее, до раздачи пользователям идентификационных номеров и секретных ключей, а не подбирается специально для проведения атак на конкретные переписки. Это условие может быть достигнуто с помощью периодической смены идентификационных номеров.

Рассмотрим модель коалиционных атак. После того, как все участники системы получили идентификационные векторы – столбцы матрицы Адамара, коалиция злоумышленников может проверить, полный набор ключей каких пользователей системы они могут составить из объединения своих ключей. Для этого они могут построить множества $I_{\{0\}}(W)$ и $I_{\{1\}}(W)$, где W – множество идентификационных номеров–столбцов злоумышленников. С помощью этих множеств они могут построить комбинаторную оболочку $< W >_{\mathcal{A}_a}$, проверив идентификационные векторы каких пользователей имеют на всех позициях из $I_{\{0\}}(W)$ нули, а на всех позициях из $I_{\{1\}}(W)$ – единицы. Если идентификационный номер пользователя попадает в комбинаторную оболочку $< W >_{\mathcal{A}_a}$, то коалиция может вычислить ключ любой переписки с его участием.

Рассмотрим теперь вероятность того, что некоторая коалиция W мощности w может получить общий секретный ключ двух произвольных участников. Будем считать, что коалиция фиксированная, а сервер распределяет идентификационные номера случайным образом.

Прежде всего опишем пространства событий, необходимые для дальнейшего рассуждения. Введем Ω^S – пространство элементарных событий, каждое из которых является одним из возможных вариантов распределения сервером идентификационных номеров между пользователями системы, $|\Omega^S| = n!$. Будем считать, что все элементарные исходы равновероятны.

Введем также Ω^T – пространство элементарных событий, каждое из которых соответствует выбору произвольной пары пользователей T, на переписку которой коалиция хочет провести атаку, $|\Omega^T| = C_n^2$. Будем как и выше считать, что все элементарные исходы равновероятны.

Рассмотрим теперь пространство $\Omega = \Omega^S \times \Omega^T$ и посчитаем вероятность наступления события, состоящего в том, что коалиция W может получить общий секретный ключ пары T. Для любого элементарного исхода $\omega = (\omega^S, \omega^T) \in \Omega$ множество столбцов, соответствующих идентификационным номерам злоумышленников из W, будем обозначать $W(\omega^S) \subset \mathcal{A}_a$, а столбцы, соответствующие идентификационным номерам пользователей из $T(\omega^T)$, будем обозначать $T(\omega^T, \omega^S) \subset \mathcal{A}_a$. По теореме 1 для того, чтобы коалиция могла получить общий ключ T необходимо, чтобы коалиция получила все ключи одного из участников T, т.е. чтобы вектор одного из участников лежал в комбинаторной оболочке векторов злоумышленников из W. Таким образом, событие, состоящее в том, что коалиция W может получить общий ключ переписки произвольной пары T, можно записать так:

$$\Omega_{\text{comp}} = \{\omega \in \Omega | < W(\omega) >_{\mathcal{A}_a} \cap T(\omega) \neq \oslash\}.$$

Отметим, что это событие можно разбить на два события:

$$\Omega_{\text{self}} = \{\omega \in \Omega | W(\omega) \cap T \neq \oslash\},$$

которое наступает в том случае, когда один из пользователей из T входит в коалицию злоумышленников из W, и

$$\Omega_{\text{at}} = \{\omega \in \Omega | W(\omega) \cap T(\omega) = \oslash \wedge < W(\omega) >_{\mathcal{A}_a} \cap T(\omega) \neq \oslash\},$$

когда коалиция может получить общий ключ T только в результате проведения коалиционной атаки.

Теперь вычислим вероятности проведения успешных коалиционных атак. Для вычисления вероятности наступления интересующего нас события Ω_{at} введем множество вспомогательных гипотез $\{H(W,r)\}_{r=1}^{w}$, которые состоят в том, что множество W имеет комбинаторный ранг r, т.е.

$$H(W,r) = \{\omega \in \Omega | \ \text{rank}_{\text{comb}}(W(\omega)) = r\}.$$

Из-за случайного распределения столбцов матрицы Адамара, т.е. идентификационных номеров системы распределения ключей, вне зависимости от выбора коалиции W множество идентификационных номеров злоумышленников $W(\omega)$ будет пробегать все возможные подмножества $\mathcal{A}_a$ мощности w. Поэтому вероятность того, что коалиция W получит множество векторов комбинаторного ранга r, т.е. выполнится гипотеза $H(W,r)$, не зависит от W, а только от мощности w. Поэтому будем записывать эту гипотезу $H(w,r)$.

Вероятность наступления гипотезы $H(w,r)$ будем вычислять рекурсивно по w и r. Множество мощности w, имеющее комбинаторный ранг $r = \text{rank}_{\text{comb}}(W)$, может быть получено из множеств мощности $w-1$, которые разбиваются на два класса: множества с комбинаторным рангом $r-1$ и множества с комбинаторным рангом r. Для этого к множеству W'_{r-1} из первого класса нужно добавить вектор, комбинаторно-независимый от всех элементов этого множества, т.е. не входящий в его комбинаторную оболочку, а к множеству W'_r из второго класса – комбинаторно-зависимый, т.е. вектор, принадлежащий комбинаторной оболочке множества, но не принадлежащий самому множеству. Таким образом, если обозначить за $|H(w,r)|$ количество элементарных исходов благоприятствующих гипотезе $H(w,r)$, то получим следующую формулу:

$$|H(w,r)| = \frac{|H(w-1,r-1)| \cdot (|\mathcal{A}_a \backslash < W'_{r-1} >_{\mathcal{A}_a}|) + |H(w-1,r)| \cdot (|< W'_r >_{\mathcal{A}_a} \backslash W'_r|)}{w} =$$

$$= \frac{|H(w-1,r-1)| \cdot (2^a - 2^{r-2}) + |H(w-1,r)| \cdot (2^{r-1} - w + 1)}{w},$$

т.к. $|\mathcal{A}_a| = 2^a$, а в силу теоремы 2 $|< W >_{\mathcal{A}_a}| = 2^{\text{rank}_{\text{comb}}(W)-1}$, причем $\text{rank}_{\text{comb}}(W'_{r-1}) = r-1$, $\text{rank}_{\text{comb}}(W'_r) = r$.

Теорема 3. *Вероятность наступления события Ω_{at} может быть вычислена по формуле:*

$$p(\Omega_{at}) = \sum_{r=1}^{w} p(\Omega_{at} | H(w,r)) \cdot |H(w,r)| / C_n^w, \tag{8}$$

$$p(\Omega_{at} | H(w,r)) = \frac{C^1_{2^{r-1}-w} \cdot C^1_{n-2^{r-1}} + C^2_{2^{r-1}-w}}{C^2_n} \tag{9}$$

Доказательство. Гипотезы $H(w,r)$, $r = 1..w$ несовместны и в сумме образуют все вероятностное пространство Ω. Применив формулу полной вероятности

$$p(\Omega_{at}) = \sum_{r=1}^{w} p(\Omega_{at}|H(w,r)) \cdot p(H(w,r)),$$

и в силу того, что $p(H(w,r)) = |H(w,r)|/C_n^w$, получим (8). Формула (9), соответствующая вероятности того, что один или оба участника переписки попали в комбинаторную оболочку коалиции при условии наступления гипотезы $H(w,r)$, естественно вычисляется по формуле гипергеометрического распределения. □

Список литературы / References

[1] Шнайер Б., *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си*, Триумф, 2002; [Schneier B., *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc., 1993.]

[2] Diffie W., Hellman M., "New Directions in Cryptography", *IEEE Transactions in Information Theory*, **22**:6 (1976), 644–654.

[3] Needham R. M. Schroeder M. D., "Using Encryption for Authentication in Large Networks of Computers", *Communications of the ACM*, **21**:12 (1978), 993–999.

[4] Matsumoto T., Imai I., "On the Key Predistribution System: A Practical Solution to the Key Distribution Problem", *CRYPTO '87 A Conference on the Theory and Applications of Cryptographic Techniques*, 1987, 185–193.

[5] Blom R., "An Optimal Class of Symmetric Key Generation Systems", *Workshop on the Theory and Applications of Cryptographic Techniques*, 1985, 335–338.

[6] Blundo C., Mattos L. A. F., Stinson D. R., "Trade-offs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution", *Annual International Cryptography Conference*, **1109** (1996), 387–400.

[7] Сидельников В. М., *Теория кодирования*, ФИЗМАТЛИТ, 2008; [Sidelnikov V. M., *Teoriya kodirovaniya*, FIZMATLIT, 2008, (in Russian).]

[8] Mitchell C. J., Piper F. C., "Key Storage in Secure Networks", *Discrete Applied Mathematics*, **21**:3 (1988), 215–228.

[9] Тарапников Ю. В., *Комбинаторные свойства дискретных структур и приложения к криптологии*, МЦНМО, 2011; [Tarannikov Yu. V., *Kombinatornye svoystva diskretnykh struktur i prilozheniya k kriptologii*, MTsNMO, 2011, (in Russian).]

[10] Stinson D. R., "On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption", *Designs, Codes and Cryptography*, **3**:12 (1997), 215–243.

[11] Stinson D. R., Trung T. V., "Some New Results on Key Distribution Patterns and Broadcast Encryption", *Designs, Codes and Cryptography*, **14** (1998), 261–279.

[12] Martin K M., "The Combinatorics of Cryptographic Key Establishment", *London Mathematical Society Lecture Note Series*, **346** (2007), 223–273.

[13] Деундяк В. М., Таран А. А., "О применении кодов Хэмминга в системе распределения ключей для конференций в многопользовательских системах связи", *Вестник ВГУ. Серия: Сист. анализ и информ. технологии*, **3** (2015), 43–50; [Deundyak V. M., Taran A. A., "O primenenii kodov Khemminga v sisteme raspredeleniya klyuchey dlya konferentsy v mnogopolzovatelskikh sistemakh svyazi", *Vestnik VGU. Seriya: Sist. analiz i inform. tekhnologii*, **3** (2015), 43–50, (in Russian).]

[14] Деундяк В. М., Таран А. А., “О вероятности проведения успешных атак на ключи конференций в полилинейных системах распределения ключей”, *Известия вузов. Сев.-Кавк. Регион. Техн. Науки*, **1** (2018), 10–17; [Deundyak V. M., Taran A. A., “O veroyatnosti provedeniya uspeshnykh atak na klyuchi konferentsy v polilineynykh sistemakh raspredeleniya klyuchey”, *Izvestiya vuzov. Sev.-Kavk. Region. Tekhn. Nauki*, **1** (2018), 10–17, (in Russian).]

[15] Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А., *Теория кодов, исправляющих ошибки*, Связь, 1979; [MacWilliams F. J., Sloane N. J. A., *The Theory of Error-Correcting Codes*, **16**, Elsevier, 1977.]

[16] Silverberg A., Staddon J., Walker J. L., “Applications of List Decoding to Tracing Traitors”, *IEEE Transactions on Information Theory*, **49**:5 (2003), 1312–1318.

Deundyak V. M., Taran A. A., "Key Distribution System Based on Hadamard Designs", *Modeling and Analysis of Information Systems*, **26**:2 (2019), 229–243.

DOI: 10.18255/1818-1015-2019-2-229-243

Abstract. The problem of key distribution in a community for providing secure communication between its participants is studied. To solve this problem, key predistribution systems can be used, in which each user receives some key information that can later be used to independently calculate required shared secret keys for conferences they participate in. Such key distribution systems can be based on different structures, such as error-correcting codes and combinatorial designs. The drawback of such systems is the possibility of collusive attacks, when traitors within the system can form a coalition and use their key information to try to calculate shared secret keys of other users. But the secrecy of keys is guaranteed by the system when the number of traitors in the coalition does not exceed a threshold defined by the system structure. In this paper, a key distribution system is based on combinatorial designs and, in particular, on Hadamard 3-design that guarantees the secrecy of communications in the presence of coalitions with less than three users. New notions of combinatorial span and combinatorial rank of a subset of Hadamard code that are required for the study of the resilience of the system to collusive attacks are introduced. The probability of successful collusive attack on an arbitrary conference against the cardinality of coalition is calculated for this system.

Keywords: key distribution systems, combinatorial designs, collusive attacks

On the authors:
Vladimir M. Deundyak, orcid.org/0000-0001-8258-2419, PhD,
Southern Federal University,
105/42 Bolshaya Sadovaya str., Rostov-on-Don 344006, Russia,
FGNU NII "Specvuzavtomatika",
51 Gazetniy lane, Rostov-on-Don 344002, Russia, e-mail: vl.deundyak@gmail.com

Alexey A. Taran, orcid.org/0000-0002-1357-9360, graduate student,
Southern Federal University,
105/42 Bolshaya Sadovaya str., Rostov-on-Don 344006, Russia, e-mail: fraktal-at@yandex.ru