О ПОСТРОЕНИИ ДИЗЪЮНКТНЫХ (SUPERIMPOSED) КОДОВ И ИХ ИСПОЛЬЗОВАНИИ В КРИПТОГРАФИИ

В.М. СИДЕЛЬНИКОВ

1. Дизъюнктные коды

Набор $\mathcal{A} = \{A_1, \ldots, A_T\}$ подмножеств множества $[N] = \{1, \ldots, N\}$ называется (w,r)-семейством непокрывающих множеств (cover-free (w,r)-family), если для него выполнены следующие свойства:

$$\bigcap_{s=1}^{w} A_{i_s} \not\subseteq \bigcup_{j=1}^{r} A_{k_j}, \text{ для всех } \{i_1, \ldots, i_w\}, \{k_1, \ldots, k_r\} \subseteq [N] \text{ таких, что } \{i_1, \ldots, i_w\} \bigcap \{k_1, \ldots, k_r\} = \varnothing \tag{1.1}$$

Идентификационная матрица $\mathfrak{K}$ (w,r)-семейством непокрывающих множеств $\mathcal{A}$, называется дизъюнктивным (w,r)-кодом. Столбцы матрицы $\mathfrak{K}$ являются идентификационными векторами множеств A_j. Таким образом, матрица $\mathfrak{K}$ имеет N строк и T столбцов. Число N обычно называется длиной дизъюнктного кода $\mathfrak{K}$, а число T называют числом его элементов. Обычно стремятся при заданных $N, (w, r)$ максимизировать число T. Семейство непокрывающих множеств и соответствующий ему дизъюнктный код — ,по существу, одно то же понятие. Эти понятия мы не будем различать.

Дизъюнктные (w,r)-коды используются для построения схем планирования экспериментов. Они находят применения и в криптографии (см., например, [7, 3], а также многие другие работы). Криптографическим приложения дизъюнктных кодов рассматриваются в п. 4 данной работы.

2. Построение дизъюнктных кодов

2.1. Конкатенантная конструкция, использующая дизъюнктный (2,q-2)-код.

Определение 2.1. *[Дизъюнктный $(2, q-2)-$ код Q_q] Пусть* $R_q^{(k)} = \{\{i+kq\}, \{i+kq, j+kq\} | i, j = 1, \ldots, q, i \neq j\}$, , $|R_q^{(k)}| = \binom{q}{2} + \binom{q}{1} = \binom{q+1}{2}$, *— множество всех двух и одноэлементных подмножеств множества* $[kq+1, (k+1)q] = \{kq+1, \ldots, kq+q\}$. *Пусть* $C_s^{(k)} = \{(s+kq, j+kq) | j = 1, \ldots, q\}$, $|C_s^{(k)}| = q$, *— множество подмножеств множества* $R_q^{(k)}$, *образованных множествами* $\{i, j\} \in R_q^{(k)}$, *которые содержат элемент* $s+kq$.

Работа выполнена при финансовой поддержке РФФИ (№02-01-00687) и NST (№CCR-0310632) во время визита автора в Мичиганский университет летом 2004 г.

Работа будет опубликована в Тезисах докладов конференции "Математика и безопастность информационных технологий", 2004, Москва, МГУ (Moscow Lomonosov University), 28-29 октября, 2004. Этот сборник выйдет в свет в начале 2005 г. на русском языке и, возможно, будет переведен на английский язык. До конца года я надеюсь послать статью под тем же названием в журнал Пробл. передачи инф. В.М. Сидельников.

Для каждого k *семейство* $\mathcal{Q}_q^{(k)} = \{C_s^{(k)} | s = 1, \dots, q\}$ *подмножеств* $\binom{q+1}{2}-$ *множества* $R_q^{(k)}$ *называется тривиальным* $(2, q-2)-$ *семейством, определенном на множестве* $(kq, (k+1)q]$. *Семейство* $\mathcal{Q}_q^{(0)}$ *обозначается как* $\mathcal{Q}_q$.

По существу, множества C_j семейства $\mathcal{Q}_q$ мы индексируем одно и двуэлементными подмножествами множества $\{1, \dots, q\}$. Поэтому дизъюнктный код, соответствующий семейству $\mathcal{Q}_q$, имееет длину $N = \binom{q+1}{2}$ (число таких подмножеств).

Каждое семейство $\mathcal{Q}_q^{(k)} = \{C_1^{(k)}, \dots, C_q^{(k)}\}, A_s^{(k)} \subset R_q^{(k)}$, содержит q элементов (подмножеств). Мощность каждого множества $C_s^{(k)}$ равна q (Обычные обозначения: $T = q$, $N = |R_q^{(k)}| = \binom{q+1}{2}$, см. [3],[4]).

Лемма 2.1. *Тривиальное* $(2, q-2)-$ *семейство* $\mathcal{Q}_q^{(k)}$ *является* $(2, q-2)-$ *семейством непокрывающих множеств. Его матрица инциденций образует* $(2, q-2)-$ *дизъюнктный код длины* $N = \binom{q+1}{2}$ *с числом элементов* q.

Доказательство. Очевидно,

$$\begin{aligned} &C_s^{(k)} \cap C_{s'}^{(k)} = \{s + kq, s' + kq\} \\ &\text{и } \{s + kq, s' + kq\} \cap (C_{s_1}^{(k)} \cup \dots \cup C_{s_{q-2}}^{(k)}) \neq \varnothing, \\ &\text{если и только если } s \in \{s_1, \dots, s_{q-2}\} \text{ или } \setminus \text{ и } s' \in \{s_1, \dots, s_{q-2}\}. \end{aligned} \tag{2.1}$$

□

Заметим, что если $k \neq k'$, то по построению $C_s^{(k)} \cap C_t^{(k')} = \varnothing$.

Если $\mathcal{A} = \{A_1, \dots, A_q\}, A_j = \{a_{j,1}, \dots, a_{j,m}\} \subset [N]$, — произвольное $(2, q-2)-$ семейство разделяющих множеств, то через $\mathcal{A}^{(k)}$ обозначается $(2, q-2)-$ семейство $\mathcal{A}^{(k)} = \{A_1^{(k)}, \dots, A_q^{(k)}\}$ разделяющих множеств, где $A_j^{(k)} = \{a_{j,1} + (k-1)N, \dots, a_{j,m} + (k-1)N\} \subset \{1 + (k-1)N, \dots, N + (k-1)N\}$.

Заметим, что если $k \neq k'$, то по построению $A_s^{(k)} \cap A_t^{(k')} = \varnothing$.

Определение 2.2 (Разделяющий код). $q-$ *значный код* $\mathfrak{K}$ *называется разделяющим* $(w, r)-$ *кодом (separating* $(w, r)-$ *code), если для любых* $\boldsymbol{y}_1, \dots, \boldsymbol{y}_w \in \mathfrak{K}$ *и любых* $\boldsymbol{x}_1, \dots, \boldsymbol{x}_r \in \mathfrak{K}$, $\{\boldsymbol{y}_1, \dots, \boldsymbol{y}_w\} \cap \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_r\} = \varnothing$, *существует компонента (координата)* $i \in [n] = \{1, \dots, n\}$ *такая, что*

$$\{y_{1,i}, \dots, y_{w,i}\} \cap \{x_{1,i}, \dots, x_{r,i}\} = \varnothing. \tag{2.2}$$

Определение 2.3. *[Конкатенантная конструкция дизъюнктного кода] Пусть* $\mathfrak{K}$ — $q-$ *значный разделяющий* $(2, r)-$ *код и* $\mathcal{A} = \{A_1, \dots, A_q\}, |A_j| = m$, $-$ $(2, q-2)-$ *семейство разделяющих множеств, содержащее* q *множеств. Семейство подмножеств* $\mathcal{A}_n(\mathfrak{K})$ *образованное подмножествами*

$$A_{\boldsymbol{x}} = A_{x_1}^{(1)} \cup A_{x_2}^{(2)} \cup \dots \cup A_{x_n}^{(n)},\ \boldsymbol{x} = (x_1, \dots, x_n) \in \mathfrak{K},\ |A_{\boldsymbol{x}}| = nq, \tag{2.3}$$

множества $\mathcal{N}_n = \cup_{k=1}^n \{(k-1) + 1, \dots, N + (k-1)N\} = \{1, \dots, nN\}$, *называется конкатенантным семейством подмножеств, порожденным разделяющим кодом* $\mathfrak{K}$ *и семейством* $\mathcal{A}$.

Число элементов (обычно обозначаемая как T*) семейства* $\mathcal{A}_n(\mathfrak{K})$ *равна* $|\mathfrak{K}|$, *число элементов* $\mathcal{N}_n$ *(длина соответствующего дизъюнктного кода) равна* $|\mathcal{N}_n| = nN$. *Если* $\mathcal{A} = \mathcal{Q}_q$, *то* $|\mathcal{N}_n| = n\binom{q+1}{2}$.

Теорема 2.1. *Пусть* $\mathfrak{K}$ — $q-$ *значный разделяющий* $(2, r)-$ *код и* $\mathcal{A} = \{A_1, \dots, A_q\}, |A_j| = m$, $-$ $(2, q-2)-$ *семейство разделяющих множеств, содержащее* q *множеств. При любом* q *семейство* $\mathcal{A}_n(\mathfrak{K})$ *является* $(2, r)-$ *семейством, непокрывающих множеств.*

Доказательство. Пусть $\boldsymbol{x}, \boldsymbol{y} \in \mathfrak{K}, \boldsymbol{x} \neq \boldsymbol{y}$. Легко видеть, что

$$A_{\boldsymbol{x}} \cap A_{\boldsymbol{y}} = (A_{x_1}^{(1)} \cap A_{y_1}^{(1)}) \cup \cdots \cup (A_{x_n}^{(n)} \cap A_{y_n}^{(n)}). \tag{2.4}$$

Пусть $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r\} \subseteq \mathfrak{K} \setminus \{\boldsymbol{x}, \boldsymbol{y}\}$. Код $\mathfrak{K}$ является разделяющим $(2,r)-$ кодом. Поэтому существует такое s, что $(x_s \notin \{x_{s,1}, \ldots, x_{s,r}\}) \& (y_s \notin \{x_{s,1}, \ldots, x_{s,r}\})$. Очевидно, из последненго соотношения и (2.1) следует

$$(A_{x_s}^{(s)} \cap A_{y_s}^{(s)}) \not\subset (A_{x_{1,s}}^{(s)} \cup \cdots \cup A_{x_{r,s}}^{(s)}). \tag{2.5}$$

Поэтому $A_{\boldsymbol{x}} \cap A_{\boldsymbol{y}} \not\subset A_{\boldsymbol{x}_1} \cup \cdots \cup A_{\boldsymbol{x}_r}$. $\square$

Следует заметить, что теорема 2.1 не совпадает с похожей теоремой, которая формулируется следующим образом (см. [3], Proposition 2.1, [4], lemma 5):

Лемма 2.2. *Пусть $\mathfrak{K}$ является $q-$ значным разделяющий $(2,r)-$ кодом с параметрами $n \times |\mathfrak{K}|$ (n — длина $\mathfrak{K}$) and B — $(2,r)-$ семейство, непокрывающих множеств (или, что одно и тоже, B — дизъюнктный $(2,r)-$ код) размера $N_1 \times q$ (q — число подмножеств в B). Тогда конкатенатный код $\mathfrak{K} \diamond B$ является дизъюнктным $(2,r)-$ кодом с параметрами $nN_1 \times |\mathfrak{K}|$.*

Замечание 2.1. *Для того, чтобы лемма 2.2 была истинна требуется, чтобы B был дизъюнктным $(2,r)-$ кодом, а $\mathfrak{K}$ — разделяющим $(2,r)-$ кодом. Теорема 2.1 показывает, что если в качестве B взять дизъюнктный $(2,q-2)-$ код $\mathcal{A}$, при то это требование при $r > q-2$ является излишне строгим. А именно, для построения дизъюнктного $(2,r)-$ кода допускается использование любого $q-$ значного разделяющего $(2,r)-$ кода, где числа q и r могут быть взяты в любой комбинации.*

Таким образом, построение дизъюнктного $(2,r)-$ кода при любом r может быть сведена к построению $q-$ значного разделяющего $(2,r)-$ кода, ибо для любого q существует $q-$ значный дизъюнктный $(2,q-2)-$ код $\mathcal{Q}_q$.

В криптографии естественно использовать дизъюнктные $(2,r)-$ коды, имеющие конкатенантную конструкцию, которые построены с помощью линейных разделяющих кодов.

3. Конструкции некоторых разделяющих и связанных с ними дизъюнктных кодов

3.1. Известная конструкция.

3.1.1. *Код Рида-Соломона как разделяющий код.*

Пусть $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_q\}$ и пусть $f = f(x) \in \mathbb{F}_q[x]$ и $\boldsymbol{a}_f = (f(\alpha_1), \ldots, f(\alpha_n))$ — вектор значений многочлена f. Код Рида-Соломона ($RS_{k,q}=$код), по определению, образован всеми векторами $\boldsymbol{a}_f$, у которых степень f не выше k, т.е.

$$RS_{k,q} = \{\boldsymbol{a}_f | deg\, f \leq k\} \tag{3.1}$$

Параметрами $q-$значного $RS_{k,q}=$кода являются (n,k,d), где $n = q$, $d = n-k+1$ и q является примарным числом.

Лемма 3.1. *(Сагалович [9],[3])*

Пусть $q > 2r$. Тогда $RS_{\left[\frac{q}{2r}\right],q}$, $|RS_{\left[\frac{n}{2r}\right],n}| = q^{\left[\frac{n}{2r}\right]+1}$, является разделяющим $(2,r)-$ кодом.

Следствие 1 (Из теоремы 2.1 и леммы 3.1). *Пусть $2r < q$. Тогда $\mathcal{Q}_{q,q}(RS_{\left[\frac{q}{2r}\right],q})$ является разделяющим $(2,r)-$ кодом при любом q.*

Скоростью передачи дизъюнктивного $(w,r)-$кода $\mathfrak{K}$ длины N называется функция

$$R(\mathfrak{K}) = \frac{\log_2 |\mathfrak{K}|}{N}. \tag{3.2}$$

Неизвестно, как построить с помощью только лемм 3.1 и 2.2, не используя теорему 2.1, бесконечную последовательность дизъюнктивных $(2,r)-$кодов, где $r = const \geq 1$, $N \to \infty$, с ненулевой скоростью. Далее мы приведем один естественный рекуррентный способ построения бесконечной последовательности $\mathfrak{K}_1, \ldots, \mathfrak{K}_m, \ldots$, подобных дизъюнктивных $(2,r)-$кодов, которая имеет в пределе нулевую скорость, но скорость стремления к нулю очень медленная.

Вместе с тем построить бесконечную последовательность конкатенантных дизъюнктивных $(2,r)-$кодов, где $r = const \geq 1$, $N \to \infty$, с ненулевой скоростью, с помощью теоремы 2.1 достаточно просто. Это будет сделано в следующем разделе.

С помощью леммы 2.2, указанная рекуррентная последовательность кодов строиться следующим образом.

Пусть $\mathfrak{K}_1$ — произвольный дизъюнктивный $(2,r)-$код длины N_1 и код $\mathfrak{K}_m$ уже построен. Пусть q_m — наибольшее примарное число такое, что $|\mathfrak{K}_m| = T_m \geq q_m$. Возьмем в качестве кода $\mathfrak{K}_{m+1}$ код $RS_{\left[\frac{q}{2r}\right],q} \diamond \mathfrak{K}_m$, который имеет длину $N_{m+1} = q_m N_m$ и число элементов $q^{\left[\frac{q_m}{2r}\right]+1}$. Покажем, что последовательность чисел $R(\mathfrak{K}_m)$ стремится к нулю.

Так как $R(\mathfrak{K}) \leq 1$, то, очевидно,

$$R(\mathfrak{K}_{m+1}) \sim \frac{log_2 q_m}{2rN_m} \sim \frac{1}{2r} R(\mathfrak{K}_m),\ m \to \infty. \tag{3.3}$$

Отсюда при любом постоянном s следует, что

$$R(\mathfrak{K}_{m+1}) \lesssim \left(\frac{1}{2r}\right)^s, \tag{3.4}$$

т.е. $\lim_{m\to\infty} R(\mathfrak{K}_m) = 0$.

Известна положительная оценка снизу величины

$$R(w,r) = \overline{\lim_{N\to\infty}} \frac{\log_2 T(N,w,r)}{N}, \tag{3.5}$$

где $T(N,w,r)$ — максимальное значение T при заданных N, w, r (см., например, [3], section 3.5). Из этой оценки следует, что существует бесконечная последовательность дизъюнктных $(2,r)-$кодов (не обязательно конкатенантных) с ненулевой скоростью.

3.2. **Построение разделяющих $(w,1)-$кодов.** В настоящем разделе мы, используя теорему 2.1, получим необходимые и достаточные условия для существования разделяющих линейных $(w,1)-$кодов.

Пусть $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$. Произведением $\boldsymbol{x} \cdot \boldsymbol{y}$ векторов $\boldsymbol{x}, \boldsymbol{y}$ является вектор

$$\boldsymbol{x} \cdot \boldsymbol{y} = (x_1 y_1, \ldots, x_n y_n). \tag{3.6}$$

Лемма 3.2. *Линейный над полем $\mathbb{F}_q$ код $\mathfrak{K}$ является разделяющим $(w,1)-$кодом тогда и только тогда, когда для любых ненулевых векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_w \in \mathfrak{K}$ выполнено*

$$\boldsymbol{x}_1 \cdots \boldsymbol{x}_w \neq 0. \tag{3.7}$$

Доказательство. Пусть $\boldsymbol{x}'_1, \ldots, \boldsymbol{x}'_w, \boldsymbol{x} \in \mathfrak{K}$, $\boldsymbol{x} \notin \{\boldsymbol{x}'_1, \ldots, \boldsymbol{x}'_w\}$.

Предположим, что для всех координат x_i у вектора $\boldsymbol{x}$ выполнено включение $x_i \in \{x'_{1,i}, \ldots, x'_{w,i}\}$, $i = 1, \ldots, n$. Тогда для векторов $\boldsymbol{x}_1 = \boldsymbol{x}'_1 - \boldsymbol{x}, \ldots, \boldsymbol{x}_w = \boldsymbol{x}'_w - \boldsymbol{x}$, принадлежащих коду $\mathfrak{K}$, соотношение (3.7) не выполняется.

Наоборот, если существует координаты x_i у вектора $\boldsymbol{x}$, для которой $x_i \notin \{x'_{1,i}, \ldots, x'_{w,i}\}$, тогда выполняется соотношение (3.7). $\square$

Лемма 3.3. *Двоичный линейный код $\mathfrak{K}$ является разделяющим $(2,1)-$ кодом, если для любых $\boldsymbol{x}, \boldsymbol{y} \in \mathfrak{K} \setminus \{0\}$*

$$wt(\boldsymbol{x}+\boldsymbol{y}) < wt(\boldsymbol{x}) + wt(\boldsymbol{y}), \tag{3.8}$$

где $wt(\boldsymbol{x})$ — вес вектора $\boldsymbol{x}$.

Доказательство. Если $\boldsymbol{x}\cdot\boldsymbol{y} = 0$, $\boldsymbol{x}, \boldsymbol{y} \in \mathfrak{K}\setminus\{0\}$, то, очевидно, $wt(\boldsymbol{x}+\boldsymbol{y}) = wt(\boldsymbol{x})+wt(\boldsymbol{y})$. $\square$

Следствие 2. *Линейный над полем $\mathbb{F}_q$ код $\mathfrak{K}$ является разделяющим $(2,1)-$ кодом, если для любого $\boldsymbol{x} \in \mathfrak{K} \setminus \{0\}$ выполнено*

$$\frac{n}{3} < wt(\boldsymbol{x}) < \frac{2n}{3}. \tag{3.9}$$

Доказательство.Если $\boldsymbol{x}\cdot\boldsymbol{y} = 0$, то $wt(\boldsymbol{x}+\boldsymbol{y}) = wt(\boldsymbol{x})+wt(\boldsymbol{y}) > \frac{2n}{3}$, что противоречит предположению следствия. $\square$

Следует сказать, что автору не известно конструктивных методов построения бесконечных семейств $q-$значных разделяющих $(w,r)-$кодов при $q = const$, $w > 1$, $n \to \infty$, которые имеют ненулевую скорость. Вместе с тем следствие 2, несмотря на свою простоту, позволяет доказать существование таких "хороших"кодов при $q = 2$.

А именно, хорошо известные методы получения границы Вашамова-Гилберта существования линейного кода с заданным кодовым расстоянием могут быть с помощью незначительных изменений трансформированы в методы получения границы существования для линейного кода, у которого ограничены снизу и свеху расстояния между парами элементов. При этом асимптотическое поведение границы не изменится.

Эта усовершенствованная граница позволяет доказать существование двоичных линейных кодов, для которых выполняется соотношение (3.9), с относительной скоростью $R = 1 - H_2\left(\frac{1}{3}\right) = 0.0817042$, что также доказывает существование линейных разделяющих $(2,1)-$ кодов.

Рассмотрим код, порождающая матрица которых является стандартной проверочной матрицей двоичного BCH-кода с удаленной единичной строкой и подходящим гарантированным кодовым расстоянием. Используя оценку А. Вейля, легко установить справедливость оценок (3.9) для таких кодов. К сожалению, этот способ позволяет построить конструктивным методом бесконечную последовательность раделяющих $(2,1)-$ кодов только с нулевой скоростью.

Заметим, что стандартными методами такими же как и для кодов, корректирующих ошибки, нетрудно получить нижние границы скорости, для которой существуют $q-$ значные разделяющие $(w,r)-$ коды длины n (см., например, [1], chapter 6). Слово "скорость"в данном случае означает скорость кода в обычном теоретико-кодовым смысле. При $q, w, r = const$, $n \to \infty$ эта скрость является положительной постоянной $R(q,w,r)$. Вместе с тем следует сказать, что эти оценки получены только кодов, которые, вообще говоря, не являются линейными.

Из теоремы 2.1 и теоремы 13 работы [1] (нижней границы существования двоичного разделяющего $(w,r)-$ кода) непосредственно вытекает

Теорема 3.1. *Существует бесконечная последовательность конкатенантных дизъюнктных $(w,r)-$ кодов для всех скоростей*

$$R(w,r) < \frac{1}{3}Y(w,r), \tag{3.10}$$

где

$$Y(w,r)=\frac{1}{w+r-1}\max_{0<p<1} log_2\left((1-p^w(1-p)^r-p^t(1-p)^w)^{-1}\right). \tag{3.11}$$

Следует сказать, что в работе [3] получены оценки $\underline{R}(w,r)$ снизу величины $R(w,r)$. В частности, $\underline{R}(2,1)=0,149$. В тоже самое время правая часть (3.10) для этого случая равна $\frac{0.2075}{3}=0.0691667$. Хотя это число заметно меньше числа $\underline{R}(2,1)$, этот результат устанавливает положительность скорости линейного двоичного разделяющего $(2,1)-$кода.

4. Схемы распределения ключей

Концепция схем распределения ключей включает следующие идеи (см. [2, 5, 7]).

1: Множество пользователей (в другой терминологии, множество вершин сети) абонентской сети связи идентифицируется с конечным множеством $\mathcal{Z}$, $|\mathcal{Z}|=T,$. Обычно $\mathcal{Z}$ является множеством чисел или множеством векторов пространства $\mathbb{F}_q^n$. В рассматриваемых ниже случаях в качестве $\mathcal{Z}$ мы рассматриваем разделяющий код $\mathfrak{K}\in\mathbb{F}_q^n$.

2: Множество $\mathcal{L}=\{k_\alpha|\alpha\in\mathcal{N}\}$ является множеством всех ключей, использующихся в абонентской сети связи. Мы полагаем, что ключи индексируются элементами множества $\mathcal{N}$. Для простоты, вместо множества $\mathcal{L}$ принято рассматривать множество $\mathcal{N}$. Обычно, число элементов $\mathcal{N}$ обозначается как $N=|\mathcal{N}|$.

3: Пусть $\mathcal{L}_{\boldsymbol{z}}=\{k_{1,\boldsymbol{z}},\dots,k_{s_{\boldsymbol{z}},\boldsymbol{z}}\}\subset\mathcal{L}$ — множество ключей пользователя $\boldsymbol{z}\in\mathcal{Z}$, которое он хранит в своей памяти (электронной). Для простоты, вместо множества $\mathcal{L}_{\boldsymbol{z}}$ мы будем рассматривать множество $\mathcal{N}_{\boldsymbol{z}}=\{(1,\boldsymbol{z}),\dots,(s_{\boldsymbol{z}},\boldsymbol{z})\}\subset\mathcal{N}$. В рассматриваемых ниже случаях в качестве $\mathcal{N}_{\boldsymbol{z}}$ мы берем множество $A_{\boldsymbol{x}}$ (см. (2.3)).

4: Множество $\mathcal{L}_{\boldsymbol{z},\boldsymbol{z}'}$ общих ключей пары пользователей $\boldsymbol{z},\boldsymbol{z}'\in\mathcal{Z}$ представляет собой множество $\mathcal{L}_{\boldsymbol{z}}\cap\mathcal{L}_{\boldsymbol{z}'}$. Вместо множества $\mathcal{L}_{\boldsymbol{z},\boldsymbol{z}'}$ мы будем рассматривать множество $\mathcal{N}_{\boldsymbol{z},\boldsymbol{z}'}=\mathcal{N}_{\boldsymbol{z}}\cap\mathcal{N}_{\boldsymbol{z}'}$. В упомянутом выше случае, в качестве $\mathcal{N}_{\boldsymbol{z},\boldsymbol{z}'}$ мы берем множество (см. (2.4))

$$\mathcal{N}_{\boldsymbol{z}}\cap\mathcal{N}_{\boldsymbol{z}'}=A_{\boldsymbol{x}}\cap A_{\boldsymbol{y}}=\bigcup_{j=1}^{n}(A_{x_j}\cap A_{y_j}). \tag{4.1}$$

5: Мы полагаем, что набор $\{\mathcal{N}_{\boldsymbol{z}}|\boldsymbol{z}\in\mathcal{Z}\}$ является $(2,r)-$семейством, разделяющих множеств, или в другой терминологии дизъюнктивным $(2,r)-$кодом.

Легко видеть, что в схеме распределения ключей, для которой выполнено это свойство, каждая коалиция $S\subset\mathcal{N},|S|\le r,$ пользователей не может получить все общие ключи пары пользователей $\boldsymbol{z},\boldsymbol{z}'\notin S$, т.е. всегда у пары $\boldsymbol{z},\boldsymbol{z}'$ имеется, по меньшей мере один общий ключ из $\mathcal{L}_{\boldsymbol{z},\boldsymbol{z}'}$, который не входит в объединение ключей недобросовестных пользователей из коалиции S. Такие схемы называются схемами распределения ключей, устойчивыми к r компрометациям.

6: Сложностью семейства, разделяющих множеств $\mathcal{N}$, или соответствующего дизъюнктного кода естественно называть число

$$a(\mathcal{N})=\max_{\boldsymbol{z}\in\mathcal{Z}}|\mathcal{N}_{\boldsymbol{z}}| \tag{4.2}$$

и минимизировать его при заданном числе T. Заметим, что этот параметр не совпадает с обще приятым параметром N — длиной дизъюнктного кода, который минимизируется во всех известных автору работах.

Например, сложность (в нашей терминологии) тривиального $(2,q-2)-$семейства Q_q равна $a(Q_q)=q$, а сложность конкатенантного семейства $\mathcal{Q}_{q,n}(\mathfrak{K})$ равна $a(\mathcal{Q}_{q,n}(\mathfrak{K}))=qn$.

Список литературы

[1] G.D. Cohen, H.G. Schaathum, Asymptotic Overview on Separating Codes, Report No 248, May 2003, Bergen, Norwey.

[2] Ch. J. Mitchell and F. C. Pipper, Key storage in secure network, Discrete Applied Mathematics, 21, 215-228, 1988.

[3] A. D'yachkov and P. Vilenkin, A. Macula and D. Torney, Families of finite sets in which no intersectin of l sets is covered by the union of s other, J. of Combinatorial Theory, S. A 99, 195-218, 2002.

[4] Hyun Kwang Kim and Vladimir Lebedev, On optimal superimposed codes.

[5] K.A.S. Quinn, Some constructions for key distribution pattens, Designs, Codes and Cryptography,4,177-191, 1994.

[6] K.A.S. Quinn, Bounds for key distribution pattens, J. Cryptology, 12, 227-239, 1999.

[7] D.R. Stinson, On some methods for unconditionally secure key distribution and broadcast encryption, Designs, Codes and Cryptography, 12, 215-243, 1997.

[8] F. W. MacWilliams and N. W. A. Sloane, The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977).

[9] Yu. L. Sagalovich, On separating systems, Problemy Peredachi Informaqtsii, 30, 14-35, 1994 (in Russian).

[10] Лебедев В.С., Асимптотическая верхняя оценка граница для скорости кодов, свободных от $(w, r)-$ перекрытий, Проблемы передачи информации, т. 39, вып. 4, 3-10, 2003.

[11] , Ким Ш.Х., Лебедев В.С., Об оптимальности тривиальных кодов, свободных от $(w, r)-$ перекрытий, Проблемы передачи информации, т. 40", №3, стр. 13-20", 2004.