Информационные процессы, Том 20, № 1, 2020, стр. 22–40.

ПЕРЕДАЧА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Теоретико-информационный подход в задаче надежного распределенного хранения информации [1]

С.А. Круглик[*,], **А.А. Фролов**[*,**]

Сколковский институт науки и технологий, Москва, Россия
Институт проблем передачи информации, Российская академия наук, Москва, Россия
Поступила в редколлегию 15.01.2020

Аннотация—В настоящее время наблюдается экспоненциальный рост объемов информации, хранимой человечеством, что, в свою очередь, увеличивает распространение распределенных систем хранения. Данные системы характеризуются, прежде всего, наличием большого числа географически распределенных серверов, что позволяет добиться хорошей масштабируемости используемых решений. При этом основными проблемами, с которыми сталкиваются их разработчики, являются временная недоступность серверов, возникающая из-за особенностей используемых в них аппаратных платформ, а также вопросы обеспечения конфиденциальности хранимой информации. В данной работе приведен обзор теоретико-информационных методов для решения данных задач, а также возможные направления дальнейших исследований в данной области

КЛЮЧЕВЫЕ СЛОВА: распределенное хранение, теоретико-информационный подход, коды с локальным восстановлением, регенерирующие коды, коды приватного восстановления информации, каналы с подслушиванием

1. ВВЕДЕНИЕ

В настоящее время мы живем в эпоху больших данных, что непосредственным образом сказывается на суммарном объеме информации, хранимой человечеством [1]. В частности, в недавних исследованиях было предсказано достижение планки в 175 зета байт хранимых данных к 2025 году [2]. При этом, ввиду удобства и простой масштабируемости, наблюдается рост популярности облачных сервисов, представляющих собой распределенный файловые системы, находящиеся на стороне провайдера услуг. Примерами таких систем являются сервисы Google disk, Облако mail.ru, Dropbox и многие другие [2, 3].

Облачные сервисы состоят из большого числа серверов, расположенных в географически распределенных дата-центрах. При этом для серверов, входящих в систему, характерны события временных отказов [4]. В частности, только в одном кластере компании Facebook, состоящем из 3000 узлов, ежедневно, по разным причинам, отказывают не менее 20 [5]. Все это заставляет операторов облачных сервисов применять методы теории кодирования для обеспечения высокой доступности данных [6, 7]. Наиболее простым и часто применяемым методом является многократное повторение данных, являющееся, по сути, простейшим кодом с повторением. Данный способ вошел в стандарт RAID-1 и широко применяется в таких системах как Apache Hadoop и Dynamo file system компании Google [8–10]. Несмотря на простоту внедрения и малую задержку при восстановлении временно недоступных данных, применение многократного повторения данных в условиях постоянного роста объема хранимой информации

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов No 18-37-00459, 19-01-00364, 19-17-50094, 19-37-90022, 20-07-00652

неприемлемо. Другим распространенным подходом является применение кодов, исправляющих стирания и являющихся более эффективными по сравнению с кодами с повторением в части избыточности. В частности, Facebok и Google применяют в своих файловых системах коды Рида-Соломона с параметрами $n = 14$, $k = 10$, $d = 5$ и $n = 9$, $k = 6$, $d = 4$ соответственно, где n обозначает длину кода, k – число информационных символов в кодовом слове, а d – кодовое расстояние в метрике Хэмминга [5, 11]. Данные коды также вошли в стандарт RAID-6 и позволяют исправлять отказы четырех и трех серверов соответственно. Несмотря на то, что случаи множественных отказов серверов в системе также возможны, наиболее частым сценарием является случай отказа одного сервера. При этом, в случае применения кодов Рида-Соломона, необходимо обратиться к k серверам, что значительным образом повышает нагрузку на систему в процессе восстановления [6, 12]. В результате возникает задача оптимального восстановления информации с временно недоступного сервера на основе избыточности, добавленной к хранимой информации. При этом существует несколько метрик эффективности вышеуказанной процедуры. Одна из них, введенная в работах [13–15], предлагает оптимизировать число серверов, участвующих в процедуре восстановления информации с временно недоступного сервера. Коды, решающие данную задачу, называются кодами с локальным восстановлением [16]. Обзору их и известных обобщений посвящен раздел 2.1. Второй популярной метрикой эффективности процедуры восстановления информации с временно недоступного сервера является суммарный объем информации, передаваемый при ее осуществлении [17]. Коды для решения данной задачи называются регенерирующими кодами. Их обзору посвящен раздел 2.2. Отметим, что каждая метрика имеет свои достоинства и недостатки, а конкретный выбор зависит, прежде всего, от типа используемой системы хранения и спектра решаемых ею задач. Обзору методов, применяемых на практике, посвящен раздел 2.3.

Другой важной проблемой, с которой сталкиваются создатели распределенных систем хранения информации, являются риски, связанные с конфиденциальностью пользовательских данных [18–20]. При этом могут рассматриваться различные модели конфиденциальности и, как следствие, методы ее обеспечения. Одной из таких моделей является постановка, при которой пользователь стремиться сохранить в секрете то, что он обратился к определенному контенту, хранимому на сервере [21]. Очевидным решением является скачивание пользователем всех данных, однако в таком случае объем скачиваемой информации может быть несоизмеримо большим. С целью оптимизации данного параметра в работе [21] было предложено рассмотреть хранение копии всех данных на нескольких серверах с использованием т.н. кодов приватного восстановления информации. Существует целый ряд работ, оптимизирующих суммарный объем информации, передаваемой пользователем в процессе доступа к интересующим его данным [22, 23]. Однако репликация данных на нескольких серверах имеет важный недостаток, связанный с увеличением объемов суммарно хранимой информации. Поэтому ее уменьшение является одним из направлений исследований задачи приватного восстановления информации [24]. Вторым важным направлением исследований является оптимизация не суммарного объема информации, передаваемого в системе, а лишь той, которую непосредственно скачивает пользователь. Данная постановка мотивирована асимметричностью между числом передаваемых и скачиваемых пользователем бит, возникающей при восстановлении больших файлов [25]. Рассмотрению данных постановок, а также их обобщений на случаи взаимодействующих серверов и серверов, неверно отвечающих на запросы пользователей, посвящен раздел 3.1. данной статьи. Второй популярной моделью конфиденциальности является постановка, при которой в системе имеется злоумышленник, обладающий полным доступом к ограниченному числу серверов. При этом информация, хранимая на серверах, закодирована с использованием кодов для борьбы с временной недоступностью сервера, а конфиденциальность понимается в теоретико-информационном смысле [26–28]. Данная постановка недавно

получила большой интерес в исследовательском сообществе, в частности в работах [29–33] рассматривается секретность в случае хранения информации с использованием кодов с локальным восстановлением, их обобщениями, а также регенерирующими кодами. Приводятся конструкции кодов, а также границы на максимальный объем информации, который можно защищенно хранить в системе. Их рассмотрению и посвящен раздел 3.2. данной статьи.

В заключении мы приводим сравнение ранее рассмотренных теоретико-информационных подходов к хранению информации в распределенных системах и описываем возможные направления дальнейших исследований.

2. ЗАДАЧА БОРЬБЫ С ВРЕМЕННОЙ НЕДОСТУПНОСТЬЮ СЕРВЕРОВ

2.1. Коды с локальным восстановлением и их обобщения

Коды, в которых каждый кодовый символ является функцией ограниченного числа других, называются кодами с локальным восстановлением. Введем ниже их формальное определение. Для этого нам потребуются некоторые предварительные сведения. Пусть $\mathbb{F}_q$ это конечное поле из q элементов и $[n] = \{1, ..., n\}$. Код $C \subseteq \mathbb{F}_q^n$ имеет локальность r если для любого кодового слова $c \in C$ и позиции i существует множество координат $R_i \subset [n] \setminus i,\ \ |R_i| \leq r$, называемое восстанавливающим множеством для координаты i, такое, что ограничение c на множество координат R_i дает возможность вычислить значение c_i. При этом в работах [14,34] были независимо выведены следующие границы на параметры данных кодов

$$R \leq \frac{r}{r+1} \tag{1}$$

$$d \leq n - k - \lceil \frac{k}{r} \rceil + 2 \tag{2}$$

Границы, учитывающие объем алфавита, полученные на основе техник укорочения, были представлены в работе [35] и имеют вид

$$k \leq \min_{1 \leq s \leq \min(\lceil \frac{n}{r+1} \rceil, \lceil \frac{k}{r} \rceil)} \{sr + k^*(n - s(r+1), d, q)\}, \tag{3}$$

где $k^*(n - s(r+1), d, q)$ – любая верхняя граница на размерность линейного кода над полем F_q длины n. Отметим, что в нелинейном случае мы можем заменить k^* на $\log_q |C|$.

Нижняя граница, полученная в работе [36] методом случайного кодирования, имеет вид

$$R_q(r, \delta) \geq 1 - \min_{o \leq s \leq 1} \{\frac{1}{r+1} \log_q((1 + (q-1)s)^{r+1} + (q-1)(1-s)^{r+1}) - \delta \log_q s\}, \tag{4}$$

где $R_q(r, \delta) = \frac{k}{n}$ – кодовая скорость, а $\delta = \frac{d}{n}$ – относительное кодовое расстояние.

Отметим, что одна из первых конструкций кодов с локальным восстановлением, оптимальных по отношению к границе (2), была представлена в работе [37]. Данная конструкция основывается на кодах в ранговой метрике и имеет экспоненциальный с длиной кода размер используемого поля. Конструкция кодов, основанная на кодах Рида-Соломона, являющаяся оптимальной по отношению к границе (2) при линейной с длиной кода размером поля была представлена в работе [38]. Для удобства читателя приведем ниже ее краткое описание.

Конструкция Тамо-Барга [38] Пусть $n \leq q$, $A \subset \mathbb{F}_q$, $|A| = n$ и для его разбиения $\mathcal{A} = \{\mathcal{A}_1, ...\mathcal{A}_{\frac{n}{r+1}}\}$ на равные подмножества существует полином $g(x)$ степени $r+1$, постоянный на каждом элементе разбиения. Перенумеруем элементы информационного вектора $a \in \mathbb{F}_q^k$ как $a_{i,j},\ \ i = 0, ...r-1,\ j = 0...\frac{k}{r} - 1$. Исходя из этого определим кодовый полином как

$$f_a = \sum_{i=0}^{r-1} \sum_{j=0}^{\frac{k}{r}-1} a_{ij} g(x)^j x^i \tag{5}$$

Кодовым словом в данном случае будет являться значение полинома (5) во всех точках множества A.

Свойство локальности при этом обеспечивается возможностью отдельной интерполяции кодового полинома внутри каждого элемента разбиения. Обобщение данной конструкции на случай циклических кодов было получено работе [39]. При этом получение циклических свойств стало возможно благодаря переходу к подгруппам мультипликативной группы поля и выбору в качестве $g(x)$ аннулирующих полиномов. Отметим, что свойства локальности классических циклических кодов стали объектом исследований работы [40], тогда как в работе [41] коды с локальностью строились с помощью выбора корней порождающего полинома. Еще одним способом построения циклических кодов с локальным восстановлением является задание порождающего полинома с помощью циклотомического полинома, описанный в статьях [42, 43]. Ввиду того, что данный подход позволяет получить оптимальные двоичные коды с локальным восстановлением для некоторого набора параметров, приведем его в данном обзоре. Для этого введем определение циклотомического полинома.

Определение 1 Для числа u, взаимно простого с p, u-ым циклотомическим полиномом над $\mathbb{F}_q$ называется полином

$$Q_u = \prod_{i=1 gcd(u,i)=1}^{u} (x - \alpha^i), \tag{6}$$

где α является u-ым примитивным корнем из единицы над $\mathbb{F}_q$ [44].

В случае, когда u и v, а также uv и q являются взаимно-простыми, определим многочлен $g_{(u,v)}(x) = (x^v - 1)Q_u(x)$. Данный многочлен, кратный многочлену $(x^v - 1)$, будет являться порождающим для кода с локальностью $u - 1$, длины uv и кодовым расстоянием 4 [43].

Конструкции оптимальных двоичных кодов с локальностью, заданные с помощью проверочных матриц описаны в работе [45]. Представленный авторами подход заключается в задании проверочной матрицы в виде $H = \begin{pmatrix} H_1 \\ H_2 \end{pmatrix}$. Строки в верхней подматрице H_1 покрывают все координаты, обеспечивая при этом выполнение свойства локальности, тогда как строки в нижней подматрице H_2 обеспечивают выполнение свойств на минимальное расстояние. После чего к полученной матрице применяется процедура укорочения. Ниже представлен пример получаемых таким образом двоичных кодов с локальным восстановлением, оптимальных с точки зрения границы (3).

Пример 1 Пусть $n = l(r + 1)$, $k = lr - \lceil \log_2(r + 1) \rceil$, $l \geq 2$, $r \geq 1$, тогда код с локальностью r и кодовым расстоянием $d = 4$ может быть задан с помощью проверочной матрицы

$$H = \begin{pmatrix} I_l \otimes i_{r+1} \\ i_l \otimes R_{r+1}, \end{pmatrix} \tag{7}$$

где i_{r+1} и i_l единичные векторы длины $r + 1$ и l соответственно. При этом

$$R_{r+1} = \left[g^{(0)}, g^{(1)}, \ldots, g^{(r)} \right],$$

где $g^{(i)}$ есть двоичное представление числа i, записанное в виде столбца длины $\lceil \log_2(r + 1) \rceil$. Отметим, что данный подход также может быть обобщен на случай q-ичных кодов с локальным

восстановлением путем замены единичного вектора в верхней подматрице на кодовое слово малого веса в двойственном МДР коде.

Отметим, что с точки зрения практических приложений, важным является построение кодов с локальностью больших длин. Из-за чего возникает задача вывода границ на максимальную длину оптимальных кодов с локальностью, рассмотренная в работе [46]. Под оптимальностью мы будем понимать достижение кодом границы (2). Тогда верхняя граница на длину оптимальных кодов с локальностью имеет вид:

$$n = \begin{cases} q + k + \lceil \frac{k}{r} \rceil - 2 & \text{если } r \geq 2 \text{ и } r|k \\ q + k + \lceil \frac{k}{r} \rceil - 2 & \text{если } r \geq 2 \text{ b } k \geq 2 \mod r \\ 2q + k + \lceil \frac{k}{r} \rceil - 2 & \text{если } r \geq 2 \text{ и } k = 1 \mod r \\ 2q + k + \lceil \frac{k}{r} \rceil - 2 & \text{если } r = 1. \end{cases} \tag{8}$$

Также в работе [46] была представлена конструкция кодов, ее достигающих. Данные коды задаются с помощью проверочной матрицы структурированной формы и для удобства читателя приведены в тексте данной статьи.

Пример 2 Для $q = 4$, $l \geq 2$, $r \geq 2$, $r \nmid k$, $k \geq 2 \bmod r$ оптимальный код с локальностью r, длина которого достигает верхнюю границу (8) задается как

$$\begin{pmatrix} I_l \otimes i_6 \\ i_l \otimes \begin{pmatrix} 010\alpha 1\alpha \\ 0011\alpha\alpha \end{pmatrix} \end{pmatrix}, \tag{9}$$

где α–примитивный элемент поля $\mathbb{F}_4$. При этом данный код имеет длину $6l$, размерность $5l-2$, локальность 5 и кодовое расстояние 4.

Естественным обобщением кодов с локальным восстановлением является рассмотрение кодов с локальным восстановлением и несколькими непересекающимися восстанавливающими множествами для каждого кодового символа. Данное свойство является особенно важным для случая т.н. "горячих данных"одновременно запрашиваемых многими пользователями, т.к. позволяет обработать их запросы в параллельном режиме. Кроме того оно открывает возможность применения техник мажоритарного декодирования для коррекции ошибок [47, 48], а также одновременного исправления нескольких стираний. Отметим, что данная область является гораздо менее исследованной, нежели чем область обычных кодов с локальным восстановлением. Границы на параметры таких кодов, а также их конструкции приведены в работах [36, 37, 49]. Введем их формальное определение.

Определение 2 Код C называется (r,t)-кодом если для любого кодового символа $i \in [n]$ существует t не пересекающихся восстанавливающих множеств $\mathcal{R}_i^1, ..., \mathcal{R}_i^t \subset [n] \setminus \{i\}$ таких, что для всех $j = 1, ...t$ и любой пары символов $a, a^{'} \in \mathbb{F}_q$, $a \neq a^{'}$ выполняется свойство

$$C(i,a)_{\mathcal{R}_i^j} \cap C(i,a')_{\mathcal{R}_i^j} = \emptyset, \tag{10}$$

где $C(i,a) = \{\mathbf{c} \in C : c_i = a\}$, $i \in [n]$.

В данном определении мы подразумеваем, что все кодовые символы обладают данным свойством. В случае же, когда код задан систематически, имеет смысл рассматривать данное свойство применительно только к информационным символам. Такие коды будем обозначать как $(r,t)_i$. Отметим, что первый класс кодов является более общим, из-за чего рассмотрим приведенные в литературе границы именно для него.

Первая граница на кодовое расстояние (r,t)-кодов была приведена в работах [50,51] и имеет вид:

$$d \leq n - k + 2 - \lfloor \frac{t(k-1)+1}{t(r-1)+1} \rfloor \tag{11}$$

В дальнейшем она была улучшена в работе [36]:

$$d \leq n - \sum_{i=0}^{t} \lfloor \frac{k-1}{r^i} \rfloor. \tag{12}$$

Последнее улучшение данной границы в явном виде было получено в работе [16] и имеет вид:

$$d \leq \min_{1 \leq i \leq k-r} \left\{ \frac{q^i - q^{i-1}}{q^i - 1} \left(n - (k-i) - \lfloor \frac{k-1-i}{r-1} \rfloor \right) \right\}, \tag{13}$$

что может быть сведено к границе

$$d \leq n - (k-1) - \lceil \frac{k-2}{r-1} \rceil, \tag{14}$$

также полученной в данной работе. Последнее же улучшение границ на кодовую скорость было получено в работе [52] и имеет вид

$$\frac{k}{n} \leq R^*_{(\mathrm{lin})}(r,t) = 1 - \frac{t}{r+t} + \frac{t}{r+1} \frac{1}{\prod_{j=1}^{r+1}(1 + \frac{1}{1+\frac{1}{j(t-1)}})}. \tag{15}$$

При этом, как и в случае кодов с локальностью, важным параметром является максимальная длина (r,t)-кодов, достигающих верхних границ на кодовое расстояние. Оценка на данный параметр, являющаяся, по своей сути, обобщением оценки из работы [46], была получена в работе [53] и для случая q-ичного (r,t)-кода с параметрами $k > r > 1$ и $d > 2$ имеет вид

$$n \leq q + k + \lceil \frac{k-2}{r-1} \rceil - 2 \tag{16}$$

Одной из первых конструкций (r,t)-кодов является обобщение конструкции Тамо-Барга на случай аннулирующих полиномов особого вида, представленное в работе [38]. Для удобства читателя приведем его в тексте статьи. Пусть существуют два разбиения $\mathcal{A}$ и $\mathcal{A}'$ подгруппы поля $A \subset \mathbb{F}_q$, $|A| = n$ на непересекающиеся множества размера $r+1$ и $s+1$ соответственно. Определим два подпространства полиномов:

$$\mathcal{F}^r_{\mathcal{A}} = \bigoplus_{i=0}^{r-1} F_{\mathcal{A}}[x] x^i \tag{17}$$

$$\mathcal{F}^s_{\mathcal{A}'} = \bigoplus_{i=0}^{s-1} F_{\mathcal{A}'}[x] x^i, \tag{18}$$

где $F_{\mathcal{A}}[x]$–множество полиномов, степени меньше $|A|$, постоянных на каждом элементе разбиения $\mathcal{A}$.

Обозначим через V_m множество полиномов, степени меньше m и входящих в пересечение пространств $\mathcal{F}_{\mathcal{A}}$ и $\mathcal{F}_{\mathcal{A}'}$. В случае, когда размер данного пересечения не меньше k, а m наименьшее число, такое что $dim(V_m) = k$, мы можем определить код как значения полинома

$\phi(a) = \sum_{i=0}^{k-1} a_i g_i(x)$ во всех точках множества A. В случае, когда разбиения $\mathcal{A}$ и $\mathcal{A}'$ ортогональные (иными словами размер пересечения их компонент не превосходит 1) данный код является кодом с локальностью $\max(r, s)$, $t = 2$, длины n, размерности k и кодовым расстоянием $n - m + 1$. Примером используемых разбиений является разбиение мультипликативной группы поля по смежным классам входящих в нее элементов [44]. Отметим, что при наличии нескольких ортогональных разбиений в структуре используемого поля мы также можем построить коды с большим значением параметра t.

Также популярным способом построения конструкций (r, t)-кодов является использование кодов произведений [50], кодов на графах [54], а также кодов на основе тензорных произведений [49]. Как правило, данные конструкции могут быть построены лишь для ограниченного числа значений параметров r и t. Одна из первых конструкций, позволяющих получить высокоскоростные двоичные коды с произвольными значениями параметров r и t, была представлена в работе [55]. Для удобства читателя приведем здесь ее описание.

Пример 2 Определим матрицу $H(m, t)$ $(m-r, t)$-кода следующим образом. Каждая строка $H(m, t)$ соответствует $(t-1)$-подмножеству $[m]$, а каждый столбец t-подмножеству $[m]$, причем подмножества строк и столбцов отсортированы в лексикографическом порядке. В этом случае элемент (i, j) матрицы $H(m, t)$ равен 1, если $E_i \subseteq F_j$, где E_i - $(t-1)$ -подмножество $[m]$, связанное с i-ой строкой, а F_j является t-подмножеством $[m]$, связанным с j-ым столбцом. В противном случае (i, j)-й элемент $H(m, t)$ равен 0. Следует отметить, что $H(m, t)$ имеет $\binom{m}{t-1}$ строк и $\binom{m}{t}$ столбцов, а также блочную структуру следующего вида.

Для $m > t > 1$:

$$H(m,t) = \begin{pmatrix} H(m-1,t-1) & 0 \\ I_{\binom{m-1}{t-1}} & H(m-1,t), \end{pmatrix} \tag{19}$$

а для $m = t$ $H(m, t) = H(m, 1)^\tau = (1, ..., 1)^\tau$. Параметры данного кода принимают следующие значения $n = \binom{r+t}{t}$, $R = \frac{r}{r+t}$ и $d = t + 1$.

Данные коды являются элементом каскадной конструкции, представленной в работе [16], которая асимптотически приближается к границам на кодовое расстояние. Отметим, что вторым элементом построенной конструкции являются коды Габидулина, позволяющие добиться хороших значений кодового расстояния, что не может быть обеспечено кодами из работы [55].

К сожалению, свойство локальности значительно уменьшает максимально достижимую кодовую скорость, что может быть неприемлемо для практических приложений. С целью борьбы с данным явлением в работе [56] было предложено рассмотрено обобщение данных кодов на случай возможного пересечения восстанавливающих множеств в небольшом числе координат, что позволяет добиться увеличения кодовой скорости при соблюдении требований на нагрузку на сервер в процессе процедуры восстановления. Отметим, что конструкции кодов, обладающих данным свойством для некоторых параметров могут быть получены с использованием $(r, \delta)_a$ кодов, представленных в работе [57]. Граница на кодовую скорость (r, t)-кодов при пересечении восстанавливающих множеств в не более чем x координатах, представленная в работе [56], имеет вид:

$$R(C) \leq R^*(r, t, x) = 1 - f(r, t, x), \tag{20}$$

где

$$f(r,t,x) = \sum_{j=1,j=1 \bmod 2}^{t} \binom{t}{j} \frac{1}{\overline{\overline{N}}(r,j,x)+1} - \sum_{j=1,j=0 \bmod 2}^{t} \binom{t}{j} \frac{1}{\underline{N}(r,j,x)+1}$$

и

$$\underline{N}(r,j,x) = \frac{(2r-(s-1)x)}{2} \min\{j, \lfloor r/x \rfloor + 1\}, \overline{N}(r,j,x) = jr.$$

Тогда как конструкции кодов, обладающих данным свойством могут быть получены с помощью повторения проверочных матриц соответствующих (r,t)-кодов.

2.2. Регенерирующие коды

Рассмотрим код C длины n над полем $\mathbb{F}_q$. Пусть данный код преобразует вектор $u \in \mathbb{F}_q^B$ в набор c_i, $i = 1, ...n$, где c_i– вектор длины α над полем $\mathbb{F}_q$, хранимый на i-ом сервере. В случае, если вектор u может быть восстановлен с помощью данных, хранящихся на любых k серверах, а данные, хранящиеся на i-ом сервере, в случае его поломки, могут быть получены с помощью любого набора из d оставшихся серверов путем скачивания с каждого из них не более чем β символов поля $\mathbb{F}_q$(эти символы являются функцией от вектора c_i, хранимого на данном сервере) данный код называется $(n,k,d,(\alpha,\beta),B)$ регенерирующим с явным восстановлением [17]. В случае же, когда результат восстановления данных, хранимых на временно недоступном сервере, является некоторой функцией от них, данные коды называются регенерирующими с функциональным восстановлением. В связи с имеющимися особенностями реализации регенерирующие коды с явным восстановлением являются наиболее интересными с практической точки зрения и именно их рассмотрению посвящен данный раздел. Отметим, что процедура восстановления может быть представлена с помощью разрезов на графе, что приводит к следующей границе на параметры регенерирующих кодов:

$$B \leq \sum_{i=0}^{k-1} \min\{\alpha, (d-i)\beta\}. \tag{21}$$

В работе [58] было показано, что данная граница даже в случае бесконечно большого числа неисправных серверов может быть достигнута с использованием линейного сетевого кодирования.

В настоящее время в большинстве работ по тематике регенерирующих кодов исследуются экстремальные точки данной границы, а именно коды с минимальной регенерацией и минимальным хранением, при этом вторые, по сути, являются кодами МДР над $\mathbb{F}_q^\alpha$ [59]. Отметим, что в случае кодов с минимальным хранением можно достичь кодовой скорости, близкой к 1, тогда как коды с минимальной регенерацией имеют ограничение в $\frac{1}{2}$, достигаемое при $k = d = n-1$, что делает их менее популярными с практической точки зрения. Приведем ниже обзор известных результатов по каждому из вышеприведенных типов кодов.

Коды с минимальным хранением

Коды, достигающие минимально возможного значения α в случае равенства в границе (21), называются кодами с минимальным хранением. Очевидно, что в этом случае $\alpha = \frac{B}{k}$,

а минимально возможное значение β равно $\frac{\alpha}{d-k+1}$. При этом суммарный объем информации $d\beta$, необходимый для восстановления временно недоступного сервера достигается в случае $d = n-1$ [60]. Важным параметром кодов, с минимальным хранением, является объем информации α, хранимой на отдельном сервере. Первая граница на данный параметр была представлена в работе [61]

$$(r+1)\log_r \alpha \le k \le l\binom{l}{\frac{l}{r}} \tag{22}$$

Нижняя граница была улучшена в работе [62]

$$2\log_2 \alpha(\log_{\frac{r}{r-1}} \alpha + 1) + 1 \ge k \tag{23}$$

Одними из первых конструкции кодов с минимальным хранением для случая низкой скорости $k \le \frac{n+1}{2}$ стали конструкции, представленные в работе [59]. В данном случае информация, хранимая на i-ом сервере, вычисляется как произведение строки Ψ_i^T кодовой матрицы Ψ на матрицу сообщения $M = [S_1\ S_2]^T$ размера $d \times \alpha$. Матрицы S_1 и S_2 являются симметричными матрицами размера $(k-1)\times(k-1)$, содержащими $B = k(k-1)$ информационных символов. При этом матрица кодирования Ψ размера $n \times d$ имеет вид $[\Phi\ \Lambda\Phi]$. Матрица Φ имеет размер $n \times (k-1)$, а матрица Λ является диагональной, составленной из n различных элементов. При этом любые d строк матрицы Ψ, а также любые α строк матрицы Φ являются линейной независимыми.

Одно из первых доказательств существования кодов с минимальным хранением и скоростью $\frac{k}{n} > 0.5$ было представлено в работе [60]. В ней авторы рассматривали случай систематических кодов с минимальным хранением и первоначально добивались выполнения свойств регенерации отдельного узла благодаря использованию порождающей матрицы специальной структуры, представленной ниже

$$G = \begin{pmatrix} I & \dots & 0 \\ & \ddots & \\ 0 & \dots & I \\ A_{1,1} & \dots & A_{1,k} \\ \vdots & \ddots & \vdots \\ A_{r,1} & \dots & A_{r,k} \end{pmatrix}. \tag{24}$$

Суммарное число серверов при этом равно $n = k + r$, где k–число серверов, хранящих информацию, а r, соответственно, проверки. Матрицы $A_{i,j}$ имеют размер $\alpha \times \alpha$. В дальнейшем, путем применения к компонентам матрицы G специальным образом выбранных матриц-перестановок достигается свойство МДР, позволяющее восстановить пользовательскую информацию путем обращения к k серверам. Отметим, что любая систематическая конструкция кодов с минимальным хранением, в том числе представленная выше, может быть приведена к несистематическому виду [63].

Явные конструкции кодов с минимальным хранением для всевозможных наборов параметров, включая $k > \frac{n+1}{2}$, на основе кодов МДР были представлены в работе [64]. Данные коды задаются с помощью проверочной матрицы размера $r \times n$, имеющей следующий вид:

$$H = \begin{pmatrix} I & \dots & I \\ A_1 & \dots & A_n \\ \vdots & \ddots & \vdots \\ A_1^{r-1} & \dots & A_n^{r-1} \end{pmatrix}, \tag{25}$$

где матрицы $A_i - A_j$ обратимы, а $A_iA_j = A_jA_i$.

Коды с минимальной регенерацией

Коды, достигающие минимально возможного значения β в случае равенства в границе (21), называются кодами с минимальной регенерацией. В данном случае параметры кода определяются как $\beta = \frac{B}{dk-\binom{k}{2}}$ и $\alpha = d\beta$. Одной из первых конструкций кодов с минимальной регенерацией в случае произвольных параметров $k \le d \le n-1$, $\beta = 1$ является конструкция, построенная на основе произведения матриц в работе [59]. В данном случае информация, хранимая на i-ом сервере, является произведением i-ой строки кодовой матрицы Ψ на матрицу сообщения M. При этом матрица $\Psi = [\phi\ \Delta]$ имеет размер $n \times d$, где матрица ϕ имеет размер $n \times k$, а матрица Δ соответственно $n \times (d-k)$. Причем любые d строк матрицы Ψ, ровно как любые k строк ϕ, линейно независимы. Матрица сообщения M является симметричной матрицей размера $d \times d$, содержащей $B = kd - \binom{k}{2}$ сообщений в виде

$$M = \begin{pmatrix} S & V \\ V^T & 0 \end{pmatrix}, \tag{26}$$

где матрица S является симметричной матрицей размера $k \times k$, а матрица V имеет размер $k \times (d-k)$.

Данный метод построения кодов с минимальной регенерацией также использовался в работе [65], в которой была оптимизирована сложность регенерации, а также исследована возможность данных кодов исправлять ошибки. Кроме того, в работе [66] были представлены коды с минимальной регенерацией для случая $d = n-1$ на основе конгруэнтного преобразования кососимметрической матрицы сообщений. Отметим, однако, что из-за существующих ограничений на кодовую скорость кодов с минимальной регенерацией они являются менее популярными у исследователей нежели коды с минимальным хранением.

2.3. Практически применяемые методы

Рост популярности облачных сервисов и, как следствие, общего числа центров обработки и хранения данных, заставляет поставщиков услуг обеспечивать высокий уровень доступности пользовательской информации. При этом, из-за особенностей применяемых решений, возможны временные отказы части используемых серверов, что может привести к временной недоступности критически важных для пользователя данных [67]. Все это приводит к применению кодовых методов в задаче распределенного хранения. На сегодняшний день наиболее простым и популярным способом является многократная репликация данных. Данный способ вошел в стандарт распределенного хранения RAID-1 и применяется в системах Apache Hadoop и Dynamo file System от Google [8–10]. Вторым наиболее популярным способом борьбы с временной недоступностью серверов является применение известных кодов, оптимизированных для исправления стираний. Данный подход вошел в стандарт распределенного хранения RAID-6 и, как правило, представлен кодами Рида-Соломона с различными параметрами [5, 11]. В частности коды (9,6) Рида-Соломона применяются в Colossus file System от Google (здесь и далее под (n, k) кодами мы понимаем коды с длиной n и числом кодовых символов k), (14,10) коды Рида-Соломона нашли свое применение в файловой системе f4 BLOB компании Facebook, Yahoo Cloud Object Store же использует (11,8) коды Рида-Соломона. Также коды Риды-Соломона используются в системах распределенного хранения компаний Baidu, Dropbox и Amazon. Еще одним способом восстановления временно недоступной информации, нашедшим свое применение на практике, является применение кодов с локальным восстановлением. В частности, в файловой системе Microscoft Azure используется (16,12) код с локальным восстановлением

с локальностью 6 построенный следующим путем добавления проверки на четность к каждой группе из 6 информационных символов и 2 проверок на четность к полученным таким образом символам [68]. К сожалению, из-за сложностей на уровне практического внедрения регенерирующие коды применяются лишь в экспериментальных системах хранения, например в системе NCCCloud [69].

3. ЗАДАЧА ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ПОЛЬЗОВАТЕЛЬСКОЙ ИНФОРМАЦИИ

3.1. Коды приватного восстановления информации

Рассмотрим классическую постановку задачи приватного восстановления информации, в которой база данных представляется в виде двоичной строки $\mathbf{x} = (x_1, ...x_n)$, а пользователь пытается получить единственный бит x_i сохраняя в секрете информацию о его индексе [21]. Очевидным решением является скачивание всей базы данных. С целью уменьшения объема скачиваемой пользователем информации в этой же работе было предложено рассмотреть репликацию базы данных на нескольких не взаимодействующих друг с другом серверах. Отметим, что в отличие от постановки с кодами для защиты от подслушивания [32, 33], серверам известно содержание пользовательских данных. Вопросы, связанные с уменьшением объемов информации, передаваемой пользователем, исследовались в целом ряде работ, в частности в работах [22, 23]. При этом основной идеей было вычисление на каждом из серверов некоторой двоичной функции от специально выбранных наборов бит. Однако главным недостатком данного подхода является многократная репликация данных, что может являться неприемлемым в случае больших баз данных. Возможным способом уменьшения суммарного объема хранимой информации является использование вычислительных схем приватного восстановления информации, в которых структура запрашиваемых пользователем данных сохраняется в секрете благодаря использованию криптографических методов, в частности односторонних функций [70]. Однако в данном обзоре рассматриваются теоретико-информационные методы, а именно протоколы и коды приватного восстановления информации. Введем их формальное определение в соответствии с работой [21].

Определение 3 k-серверный протокол приватного восстановления состоит из трех алгоритмов:

- Алгоритм $\mathcal{Q}$ генерации запросов $q_1, ...q_k$ к серверам
- Алгоритм $\mathcal{A}$ ответа сервера $a_j = \mathcal{A}(k, j, \mathbf{x}, q_j)$
- Алгоритм $\mathcal{C}$ реконструкции запрашиваемого бита x_i на основе ответа серверов $a_1, ...a_k$

При этом данный протокол должен обеспечивать корректное восстановление запрашиваемой информации, а также обладать свойствами приватности, выражающимися в независимости распределения запросов к серверам $q_1, ...q_k$ от запрашиваемого бита.

Отдельно отметим, что все существующие на данный момент k-серверные протоколы приватного восстановления являются линейными, что означает выполнение свойства $\mathcal{A}(k, j, \mathbf{x}_1 + \mathbf{x}_2, q_j) = \mathcal{A}(k, j, \mathbf{x}_1, q_j) + \mathcal{A}(k, j, +\mathbf{x}_2, q_j)$

Определение 4 Код C называется k-серверным кодом приватного восстановления, если для каждого информационного бита существует k непересекающхся наборов кодовых бит, таких что он является функцией каждого из них.

Отметим, что данное определение является схожим с (r, t)-кодами, но с той лишь разницей, что в данном случае мы не ограничиваем размер восстанавливающего множества для каждого символа.

При наличии k-серверного протокола приватного восстановления и k-серверного кода приватного восстановления длины m и размерности s мы можем создать теоретико-информационную схему приватного восстановления информации следующим образом:

1. Разделим двоичную строку $\mathbf{x}$ длины n на s частей длины $\frac{n}{s}$
2. Закодируем ее с помощью имеющегося кода в строку $\mathbf{c}$ длины m, компоненты которой имеют длину $\frac{n}{s}$ и хранятся на m невзаимодействующих серверах
3. Для восстановления i-го бита из l-ой части двоичной строки $\mathbf{x}$ $(x_{l,i})$ пользователь генерирует k запросов $q_1, ...q_k$ с помощью имеющегося протокола
4. Пользователь находит k непересекающихся восстанавливающих множеств $\mathcal{R}_1, ...\mathcal{R}_k$ l-ой части исходной двоичной строки x_l
5. Для любого j, входящего в объединение $\mathcal{R}$ данных восстанавливающих множеств, пользователь находит такое уникальное число t, что $j \in \mathcal{R}_t$ и формирует запрос к серверу j как q_t. Запросы же к другим серверам могут быть взяты произвольно т.к. их ответы будут проигнорированы
6. Пользователь получает ответы с серверов $j \in \mathcal{R}$ и вычисляет $a_t^{'} = \sum_{j \in \mathcal{R}_t} \mathcal{A}(k, t, \mathbf{c}_j, q_t) = \mathcal{A}(k, t, \mathbf{x}_l, q_t)$ используя свойство линейности протокола
7. Пользователь вычисляет запрашиваемый бит $x_{l,i}$ как $\mathcal{C}(k, \frac{n}{s}, i, a_1^{'}, ...a_k^{'})$

В случае, если число загружаемых пользователем бит используемого k-серверного протокола приватного восстановления для базы данных длины n в наихудшем случае составляет $U(n)$, а число скачиваемых данных, также в наихудшем случае, составляет $D(n)$, то число бит, загружаемых в случае вышеописанной схемы не превосходит $\frac{m}{k}U(\frac{n}{s}) + m \log k$, а число скачиваемых данных не превосходит $\frac{m}{k}D(\frac{n}{s})$. При этом важным параметром используемой схемы является суммарная избыточность, определяемая избыточностью используемого кода приватного восстановления. Из-за чего возникает задача построения k-серверных кодов приватного восстановления с малой избыточностью. Как правило данные коды строятся на основе имеющихся методов теории кодирования. Рассмотрим пример таких кодов, основанный на геометрии многомерных кубов и представленный в работе [71].

Пример 3 Пусть (m, s) k-серверный код приватного восстановления $C_a(\sigma, k)$ имеет $s = \sigma^{k-1}$ информационных бит, обозначаемых через $x_{i_1,...i_{k-1}}$, где $1 \leq i_j \leq \sigma$, $j = 1, ...k-1$. Разделим $(k-1)\sigma^{k-2}$ проверочных бит на $k-1$ групп и определим их как

$$p^{\varepsilon}_{i_1,..i_{\varepsilon-1},i_{\varepsilon+1},...i_{k-1}} = \sum_{i_\varepsilon=1}^{\sigma} x_{i_1,...i_{k-1}}, \tag{27}$$

где $\varepsilon = 1, ...k-1$.

Полученный таким образом код будет являться k-серверным кодом приватного восстановления. Также в данной статье были представлены коды приватного восстановления на основе систем Штейнера, кодов постоянного веса и кодов с мажоритарной логикой. В работе [72] были получены коды приватного восстановления информации на основе укороченных кодов Рида-Малера в проективных пространствах.

Отметим, что в оригинальной постановке задачи предполагалось, что рассматриваемые файлы имеют размер один бит, а база данных является битовой строкой. Однако с практической точки зрения наиболее интересен случай файлов произвольного размера. В данном случае объем информации, загружаемой пользователем при восстановлении файла может быть несоизмеримо мал по сравнению с объемами скачиваемой информации. Поэтому возникает задача оптимизации именно числа скачиваемых пользователем бит, поставленная в работе [25]. Данная постановка позволяет ввести параметр, называемой скоростью приватного восстановления,

являющейся отношением размера восстановленного файла и суммарного объема скачанной информации. Супремум по всевозможным достижимым скоростям приватного восстановления по всем достижимым схемам приватного восстановления называется пропускной способностью приватного восстановления. В случае, когда каждый из k серверов хранит все n файлов данный параметр имеет вид $C = \frac{1-k^{-n}}{1-k^{-1}}$. В случае же использования в схеме k-серверного кода приватного восстановления, являющегося (m, s) МДР кодом, удается достичь пропускной способности $C = \frac{1-(s/m)^n}{1-s/m}$ [73].

При этом в литературе существует большое число обобщений постановок задачи приватного восстановления информации (как в случаях простой репликации базы данных на каждом сервере, так и в случаях применения кодов приватного восстановления) на различные случаи некорректного поведения серверов. Примерами такого некорректного поведения является взаимодействие t серверов [74], временный отказ некоторых из них [74], а также ответ части серверов с ошибкой [73], утечки части передаваемых в процессе работы схемы данных [75] и их различные комбинации. Отметим, что устойчивость к такому поведению достигается как путем модификации протокола приватного восстановления, так и кодов приватного восстановления при их использовании. При этом пропускная способность таких схем для многих случаев до сих пор остается неизвестной.

3.2. Коды для защиты от подслушивания

Рассмотрим задачу обеспечения теоретико-информационной безопасности пользовательских данных, хранимых в распределенной системе при наличии пассивного злоумышленника способного читать часть информации. Введем формальное определение. Пусть хранимые в системе пользовательские данные S закодированы в кодовые символы C, распределенные по n серверам. Рассмотрим пассивного злоумышленника, имеющего доступ к части хранимой информации, выражаемой как $E(C)$. При этом под $E(C)$ могут пониматься как все данные, хранимые на l_1 серверах, так и их часть (или какая-то функция от них). Кроме того злоумышленнику также могут быть доступны данные, передаваемые в процессе восстановления l_2 временно недоступных серверов. Тогда под теоретико-информационной защищенностью пользовательских данных понимается равенство нулю взаимной информации между S и $E(C)$, т.е. условие $I(S; E(C)) = 0$. Впервые данная постановка возникла при исследовании каналов с прослушиванием, первоначально введенных в работе [76], а затем обобщенных в [77]. В случае последних предполагается, что злоумышленник самостоятельно определяет доступную ему информацию $E(C)$. В работе [77] были приведены нижние оценки на энтропию информации пользователя и информации, доступной злоумышленнику, $H(S, E(C))$, полученные с помощью случайного кодирования и кодирования в смежных классах. Последнее заключается в представлении пользовательской информации в виде случайного вектора смежного класса некоторого линейного кода. Также авторами были получены верхние оценки на величину $H(S, E(C))$, которые в дальнейшем были связаны с понятием обобщенных весов Хэмминга в работе [78]. В частности было показано, что иерархия обобщенных весов Хэмминга определяет точки изменения кривой на графике $H(S, E(C))$ от E. Отметим, что существующие конструкции для таких каналов используют как кодирование в смежных классах, так и предварительное кодирование информационных и случайных бит с помощью кодов с максимальным кодовым расстоянием. При этом, в случае применения данных подходов к задаче распределенного хранения полученная с их помощью информация кодируется с использованием одного из кодов раздела 2 [32, 33]. Формально данные конструкции могут быть описаны с помощью порождающей матрицы кода, имеющей вид

$$G = \begin{pmatrix} G_1 \\ G_2 \end{pmatrix}, \tag{28}$$

причем матрица G_1 соответствует информационным символам, а матрица G_2 добавляемым к ним случайным.

Одной из первых конструкций регенерирующих кодов, устойчивых к злоумышленнику с доступом к l_1 серверам, а также данным, передаваемым при восстановлении l_2 временно недоступных серверов является конструкция на основе произведения матриц [79]. В данной работе рассматривались как коды с минимальной регенерацией, так и коды с минимальным хранением, описанные в соответствующих подразделах раздела 2.2. При этом в случае последних, ввиду хранения восстанавливающим узлом всех данных, загружаемых во время восстановления, мы можем, не теряя общности, принять $l_2 = 0$. В данном случае мы заменяем $l_1 d - \binom{l}{2}$ информационных символов на случайные в первых l_1 строках симметричной матрицы M. Если при этом в ограничении матрицы Ψ на первые l_1 столбцов любые l_1 строк будут линейно независимы, то данный метод кодирования обеспечивает устойчивость к злоумышленнику, имеющему доступ к данным, хранимых на l_1 серверах. В случае кодов с минимальной регенерацией заменим $R = (l_1 + l_2)\alpha + (k - (l_1 + l_2)l_2$ символов на случайные следующим образом. Заменим $(l_1 + l_2)\alpha - \binom{l_1+l_2}{2}$ символов в первых $l_1 + l_2$ строках и столбцах матрицы S_1, $\binom{l}{2}$ символов на пересечении первых l_1+l_2-1 строк и столбцов матрицы S_2 и $(k-l_1-l_2)l_2$ оставшихся символов в первых l_2 строках и столбцах матрицы S_2 на случайные с сохранением свойств симметрии. В случае, когда в ограничении матрицы Ψ на первые l_1+l_2 столбцов любые l_1+l_2 строк будут линейно независимы, данный метод кодирования обеспечивает устойчивость к злоумышленнику, имеющему доступ к данных, хранимых на l_1 серверах, а также скачиваемых в процессе восстановления l_2 временно недоступных серверов. Конструкции на основе предварительного кодирования информационных и случайных бит с использованием кодов Габидулина, а также кодирования в смежных классах были представлены в работах [31, 33]. Важным параметром данных кодов является максимально возможный объем хранимой информации. В работе [80] было показано, что объем пользовательских данных B^* ограничен сверху как

$$B^* \leq \sum_{i=l_1+l_2}^{k-1} \min(\alpha, (d-i)\beta) \tag{29}$$

При этом в случае кодов с минимальной регенерацией данная граница принимает форму

$$B^* \leq (kd - \frac{k(k-1)}{2})\beta - (l_1 d - \frac{l_1(l_1-1)}{2})\beta \tag{30}$$

В случае же кодов с минимальным хранением улучшение данной границы было получено в работе [31] и имеет вид

$$B^* \leq (k - l_1 - l_2)(\alpha - \beta) \tag{31}$$

Явные конструкции кодов с минимальной регенерацией для всех наборов параметров, а также кодов с минимальным хранением для случая $l_2 \leq 1$, оптимальные с точки зрения вышеописанных границ были представлены в работе [80].

В случае кодов с локальным восстановление одна из первых конструкций, устойчивых к злоумышленнику, имеющему доступ к l_1 серверам была представлена в работе [32]. В ней к информационному вектору добавлялись l_1 случайных символов, затем полученный вектор кодировался кодом Габидулина скорости 1, а уже затем к полученным символам применялся код с локальным восстановлением. В данной работе была показана эквивалентность

теоретико-информационной защищенности условию линейной независимости строк матрицы G_2, соответствующих l_1 линейно-независимым строкам матрицы G, а также его выполнение в случае применения предварительного кодирования с использованием кодов Габидулина. В работах [31, 33] данная задача была расширена на случай устойчивости к злоумышленнику, имеющему доступ не только к l_1 серверам, но и данным, передаваемыми при восстановлении l_2 серверов. Для обеспечения теоретико-информационной защищенности в работе [33] использовалось предварительное кодирование с использованием кодирования в смежных классах. Граница на максимально возможный объем информации была получена в работах [31, 32] и имеет вид

$$B^* \leq m - \lfloor \frac{n - d_{min} + 1}{r + 1} \rfloor - l_1 - rl_2 \tag{32}$$

Данная граница может быть достигнута в случае использования в вышеописанных конструкциях оптимальных кодов с локальным восстановлением.

4. ЗАКЛЮЧЕНИЕ

В настоящей работе нами были рассмотрены возможные способы решения задач, возникающих в случае распределенного хранения информации с помощью теоретико-информационного подхода. К сожалению, из-за имеющихся сложностей реализации свое применение на практике, и то, в достаточно ограниченном виде, нашли лишь коды с локальным восстановлением. Одним из наиболее перспективных направлений исследований в данной области, по мнению авторов, является уменьшение вычислительной сложности используемых методов, а также переход к двоичным полям, что откроет дорогу их практическому применению.

Данный обзор является отражением мнения авторов на данную бурно развивающуюся область теории информации и не претендует на полноту ввиду огромного числа работ в ней, в особенности вышедших в последние 10 лет.

СПИСОК ЛИТЕРАТУРЫ

1. U. Aftab and G. F. Siddiqui, "Big Data Augmentation with Data Warehouse: A Survey", 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 2785-2794.

2. David Reinsel,John Gantz, John Rydning, "The Digitization of the World From Edge to Core", An IDC White Paper ? #US44413318, 2018.

3. C. Li and C. Yang, A Novice, "Group Sharing Method for Public Cloud:, 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 966-969.

4. W. Hai-Jia, L. Peng and C. Wei-Wei, "The Optimization Theory of File Partition in Network Storage Environment", 2010 Ninth International Conference on Grid and Cloud Computing, Nanjing, 2010, pp. 30-33.

5. M. Sathiamoorthy et al., "XORing elephants: Novel erasure codes for big data", Proc. Very Large Data Bases Endowment, vol. 6, no. 5, pp. 325?336, Mar. 2013.

6. Balaji, S.B., Krishnan, M.N., Vajha, M. et al., "Erasure coding for distributed storage: an overview", Sci. China Inf. Sci. (2018) 61: 100301.

7. N. Rakesh, V. Tyagi, "Failure recovery in XOR'ed networks", in 2012 IEEE International Conference on Signal Processing, Computing and Control (ISPCC-2012), 2012

8. H. Weatherspoon and J. D. Kubiatowicz, "Erasure coding vs. replication: a quantitiative comparison", in Proc. IPTPS, 2002.

9. R. Rodrigues and B. Liskov, "High availability in DHTs: Erasure coding vs. replication", in Proc. IPTPS, 2005.

10. B.-G. Chun, F. Dabek, A. Haeberlen, E. Sit, H. Weatherspoon, M. F. Kaashoek, J. Kubiatowicz, and R. Morris, "Efficient replica maintenance for distributed storage systems", in NSDI, 2006.

11. H. Dau et al, "Repairing Reed-Solomon Codes with Single and Multiple Erasures", ITA, 2017, San Diego.

12. J. Li and B. Li, "Erasure coding for cloud storage systems: A survey", Tsinghua Science and Technology, vol. 18, no. 3, pp. 259?272, 2013.

13. J. Han, L. Lastras-Montano, "Reliable memories with subline accesses", in Proc. ISIT, 2007, pp. 2531-2535.

14. C. Huang, M. Chen, J. Li, "Pyramid codes: Flexible schemes to trade space for access efficiency in reliable data storage systems", ACM Transactions on Storage (TOS), vol. 9, no. 1, pp. 3, 2013.

15. P. Gopalan, et al. "On the locality of codeword symbols." IEEE Trans. Inform. Theory, vol. 58, no. 11, pp. 6925-6934, 2012

16. S. Kruglik, K. Nazirkhanova and A. Frolov, "New Bounds and Generalizations of Locally Recoverable Codes With Availability", in IEEE Trans. Inform. Theory, vol. 65, no. 7, pp. 4156-4166, 2019.

17. A. Dimakis, P. Godfrey, Y. Wu, M. Wainwright, K. Ramchandran, "Network coding for distributed storage systems", IEEE Trans. Inform. Theory, vol. 56, no. 9, pp. 4539-4551, 2010.

18. Rouayheb, S., Goparaju, S., and Ramchandran, K., Security in Distributed Storage Systems. In R. Schaefer, H. Boche, A. Khisti, and H. Poor (Eds.), "Information Theoretic Security and Privacy of Information Systems", Cambridge: Cambridge University Press, pp. 519-553, 2017.

19. Minowa T., Takahashi T. "Secure Distributed Storage for Bulk Data", In: Huang T., Zeng Z., Li C., Leung C.S. (eds) Neural Information Processing. ICONIP 2012. Lecture Notes in Computer Science, vol 7667. Springer, Berlin, Heidelberg

20. Vishal Kher, and Yongdae Kim, "Securing distributed storage: challenges, techniques, and systems", In Proceedings of the 2005 ACM workshop on Storage security and survivability (StorageSS '05), ACM, New York, NY, USA, 9-25, 2005.

21. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval", J. ACM, 45, 1998.

22. K. Efremenko, "3-query locally decodable codes of subexponential length", Proc. of the 36-th Annual ACM Symposium on Theory of Computing, pp. 39-44, Bethesda, MD, June 2009.

23. S. Yekhanin, "Towards 3-query locally decodable codes of subexponential length", Joural ACM, vol. 55, no. 1, pp. 1-16, 2008.

24. N. B. Shah, K. V. Rashmi, and K. Ramchandran, "One extra bit of download ensures perfectly private information retrieval", Proc. IEEE Int. Symp. on Inform. Theory, pp. 856-890, Honolulu, HI, June-July 2014.

25. T. H. Chan, S.W. Ho, and H. Yamamoto, "Private Information Retrieval for Coded Storage", Proc. IEEE Int. Symp. on Inf. Theory, pp. 2842-2846, Hong Kong, Jun. 2015.

26. C. E. Shannon, "Communication theory of secrecy systems", Confidential report, 1946.

27. A. D. Wyner, "The wire-tap channel", Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355?1387, Oct. 1975.

28. I. Csiszar and J. Korner, "Broadcast channels with confidential messages", IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339?348, May 1978.

29. S. Pawar, S. E. Rouayheb, and K. Ramchandran, "Securing Dynamic Distributed Storage Systems Against Eavesdropping and Adversarial Attacks", IEEE Trans. Inf. Theory, vol. 57, no. 10, pp. 6734?6753, Oct. 2011.

30. S. Goparaju, S. E. Rouayheb, R. Calderbank, and H. V. Poor, "Data secrecy in distributed storage systems under exact repair", in International Symposium on Network Coding (NetCod), June 2013, pp. 1?6.

31. A. Rawat, O. Koyluoglu, N. Silberstein, and S. Vishwanath, "Optimal locally repairable and secure codes for distributed storage systems", IEEE Trans. Inform. Theory, vol. 60, no. 1, pp. 212?236, Jan 2014.

32. A. Agarwal and A. Mazumdar, "Security in locally repairable storage", IEEE Trans. Inform. Theory, vol. 62, no. 11, pp. 6204? 6217, Nov 2016.

33. S. Kadhe and A. Sprintson, "Security for minimum storage regenerating codes and locally repairable codes", In Proc. 2017 IEEE ISIT, Aachen, 2017, pp. 1028-1032.

34. D. S. Papailiopoulos and A. G. Dimakis, "Locally repairable codes," In Proc. 2012 IEEE ISIT, Cambridge, MA, 2012, pp. 2771-2775.

35. V. Cadambe and A. Mazumdar, ?Upper bounds on the size of locally recoverable codes,? IEEE Trans. Inform. Theory, vol. 61, no. 8, pp. 5787?5794, 2015.

36. I. Tamo, A. Barg and A. Frolov, "Bounds on the Parameters of Locally Recoverable Codes," in IEEE Trans. Inform. Theory, vol. 62, no. 6, pp. 3070-3083, June 2016.

37. N. Silberstein, A. S. Rawat, O. Koyluogly, and S. Vishwanath, ?Optimal locally repairable codes via rank-metric codes,? in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jul. 2013, pp. 1819?1823.

38. I. Tamo and A. Barg, "A Family of Optimal Locally Recoverable Codes," in IEEE Trans. Inform. Theory, vol. 60, no. 8, pp. 4661-4676, Aug. 2014.

39. I. Tamo, A. Barg, S. Goparaju, and R. Calderbank, ?Cyclic LRC codes and their subfield subcodes,? in IEEE Int. Symp. Inform. Theory, Hong Kong, Jun. 2015, pp. 1262?1266

40. P. Huang, E. Yaakobi, H. Uchikawa, and P. H. Siegel, ?Cyclic linear binary locally repairable codes,? in IEEE Inform. Theory Workshop (ITW), Jerusalem, Israel, Apr. 2015, pp. 1 ? 5.

41. A. Zeh and E. Yaakobi, "Optimal linear and cyclic locally repairable codes over small fields," In Proc. 2015 IEEE ITW, Jerusalem, 2015, pp. 1-5.

42. C. Kim and J.-S. No, ?New constructions of binary and ternary locally repairable codes using cyclic codes,? IEEE Commun. Lett., vol. 22, no. 2, pp. 228?231, Feb. 2018.

43. P. Tan, Z. Zhou, H. Yan and U. Parampalli, "Optimal Cyclic Locally Repairable Codes via Cyclotomic Polynomials," in IEEE Communications Letters, vol. 23, no. 2, pp. 202-205, Feb. 2019.

44. R. Lidl and H. Niederreiter, "Finite Fields", vol. 20. Cambridge, U.K.: Cambridge Univ. Press, 1997.

45. J. Hao, S. Xia and B. Chen, "Some results on optimal locally repairable codes," In Proc. 2016 IEEE ISIT, Barcelona, 2016, pp. 440-444.

46. J. Hao, K. Shum, S. Xia and Y. Yang, "On the Maximal Code Length of Optimal Linear Locally Repairable Codes," In Proc. 2018 IEEE ISIT, Vail, CO, 2018, pp. 1326-1330.

47. Берлекэмп Э., "Алгебраическая теория кодирования," М.: Мир, 1971, пер. с англ.

48. A. Singh Rawat, D. S. Papailiopoulos and A. G. Dimakis, "Availability and locality in distributed storage," 2013 IEEE Global Conference on Signal and Information Processing, 2013, pp. 923-928.

49. P. Huang, E. Yaakobi, H. Uchikawa, and P. H. Siegel, ?Linear locally repairable codes with availability,? in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2015, pp. 1871?1875

50. A. Wang and Z. Zhang, ?Repair locality with multiple erasure tolerance,?IEEE Trans. Inf. Theory, vol. 60, no. 11, pp. 6979?6987, Nov 2014.

51. A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, ?Locality and availability in distributed storage,? In Proc. 2014 IEEE ISIT, June 2014, pp. 681?685

52. S. B. Balaji and P. V. Kumar, ?Bounds on the rate and minimum distance of codes with availability,? in Proc. 2017 IEEE ISIT, June 2017, pp. 3155?3159.

53. S. Kruglik, K. Nazirkhanova and A. Frolov, "On the Maximal Code Length of Optimal Linear LRC Codes with Availability," 2018 Engineering and Telecommunication (EnT-MIPT), Moscow, 2018, pp. 54-57.

54. N. Prakash, V. Lalitha, and P. Kumar. ?Codes with locality for two erasures,? in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Honolulu, 2014, pp. 1962?1966.

55. A. Wang, Z. Zhang and M. Liu, "Achieving arbitrary locality and availability in binary codes," In Proc. 2015 IEEE ISIT, Hong Kong, 2015, pp. 1866-1870.

56. S. Kruglik, M. Dudina, V. Potapova and A. Frolov, "On one generalization of LRC codes with availability," In Proc. 2017 ITW, Kaohsiung, 2017, pp. 26-30.

57. N. Prakash, G. M. Kamath, V. Lalitha, and P. V. Kumar, ?Optimal linear codes with a local-error-correction property,? in2012 IEEE InternationalSymposium on Information Theory Proceedings, July 2012, pp. 2776?2780.

58. Y. Wu, "Existence and construction of capacity-achieving network codes for distributed storage," In Proc. 2009 IEEE ISIT, Seoul, 2009, pp. 1150-1154.

59. K. V. Rashmi, N. B. Shah and P. V. Kumar, "Optimal Exact-Regenerating Codes for Distributed Storage at the MSR and MBR Points via a Product-Matrix Construction," in IEEE Trans. Inform. Theory, vol. 57, no. 8, pp. 5227-5239, Aug. 2011.

60. S. Goparaju, A. Fazeli and A. Vardy, "Minimum Storage Regenerating Codes for All Parameters," in IEEE Trans. Inform. Theory, vol. 63, no. 10, pp. 6318-6328, Oct. 2017.

61. I. Tamo, Z. Wang and J. Bruck, "Access Versus Bandwidth in Codes for Storage," in IEEE Trans. Inform. Theory, vol. 60, no. 4, pp. 2028-2037, April 2014.

62. S. Goparaju, I. Tamo and R. Calderbank, "An Improved Sub-Packetization Bound for Minimum Storage Regenerating Codes," in IEEE Trans. Inform. Theory, vol. 60, no. 5, pp. 2770-2779, May 2014.

63. J. Li, X. Tang and C. Tian, "A generic transformation for optimal repair bandwidth and rebuilding access in MDS codes," In Proc. 2017 IEEE ISIT, Aachen, 2017, pp. 1623-1627.

64. M. Ye and A. Barg, "Explicit Constructions of High-Rate MDS Array Codes With Optimal Repair Bandwidth," in IEEE Trans. Inform. Theory, vol. 63, no. 4, pp. 2001-2014, April 2017.

65. Y. S. Han, H. Pai, R. Zheng and P. K. Varshney, "Update-Efficient Error-Correcting Product-Matrix Codes," in IEEE Transactions on Communications, vol. 63, no. 6, pp. 1925-1938, June 2015.

66. S. Lin and W. Chung, "Novel Repair-by-Transfer Codes and Systematic Exact-MBR Codes with Lower Complexities and Smaller Field Sizes," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 12, pp. 3232-3241, Dec. 2014.

67. R. Miller, "Inside Amazon?s cloud computing infrastructure, Data Center Frontier", 2015. [Online]. Available: http://datacenterfrontier.com/ inside-amazon-cloud-computing-infrastructure/

68. C. Huang, H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li, and S. Yekhanin, ?Erasurecoding in Windows Azure storage,? USENIX Annual Technical Conference (ATC), 2012

69. Yuchong Hu, Henry C. H. Chen, Patrick P. C. Lee, and Yang Tang "NCCloud: Applying Network Coding for the Storage Repair in a Cloud-of-Clouds" Proceedings of the 10th USENIX Conference on File and Storage Technologies (FAST '12), San Jose, CA, February 2012.

70. E. Kushilevitz and R. Ostrovsky, "Replication is not needed: Single database, computationally-private information retrieval", Proc. 38-th IEEE Symp. Foundations Computer Science, pp. 364?373, October 1997.

71. A. Fazeli, A. Vardy, and E. Yaakobi, ?PIR with low storage overhead: Coding instead of replication,? CoRR, vol. abs/1505.06241, 2015.

72. M. Vajha, V. Ramkumar, and P. V. Kumar, ?Binary, shortened projective Reed Muller codes for coded private information retrieval,? in Proc. IEEE Int. Symp. Inf. Theory, Aachen, Germany, Jun. 25?30, 2017, pp. 2648?2652.

73. K. Banawan and S. Ulukus, "The Capacity of Private Information Retrieval From Coded Databases," in IEEE Trans. Inform. Theory, vol. 64, no. 3, pp. 1945-1956, March 2018.

74. H. Sun and S. A. Jafar, "Blind interference alignment for private information retrieval," In Proc. 2016 IEEE ISIT, Barcelona, 2016, pp. 560-564.

75. Q. Wang and M. Skoglund, "Secure Private Information Retrieval from Colluding Databases with Eavesdroppers," In Proc. 2018 IEEE ISIT, Vail, CO, 2018, pp. 2456-2460.

76. A. D. Wyner, "The wire-tap channel," in The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

77. L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in AT&T Bell Laboratories Technical Journal, vol. 63, no. 10, pp. 2135-2157, Dec. 1984.

78. V. K. Wei, "Generalized Hamming weights for linear codes," in IEEE Trans. Inform. Theory, vol. 37, no. 5, pp. 1412-1418, Sept. 1991.

79. N. B. Shah, K. V. Rashmi and P. V. Kumar, "Information-Theoretically Secure Regenerating Codes for Distributed Storage," 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, Houston, TX, USA, 2011, pp. 1-5.

80. K. V. Rashmi, N. B. Shah, K. Ramchandran and P. V. Kumar, "Information-Theoretically Secure Erasure Codes for Distributed Storage," in IEEE Trans. Inform. Theory, vol. 64, no. 3, pp. 1621-1646, March 2018.

An information-theoretic approach for reliable distributed storage systems

S.A. Kruglik, A.A. Frolov

Nowadays exponential growth of the total amount of data stored by humanity leads to the expansion of distributed storage systems. Such systems have a huge amount of geographically distributed servers that give good scalability. The main challenges with such systems are the temporary unavailability of servers due to features of hardware inside them as well as confidentiality issues. In this article we consider the information-theoretic approach to solve these issues and give possible further research direction in this area

KEYWORDS: distributed storage, information-theoretic approach, locally recoverable codes, regenerating codes, PIR, wiretap channels

ACKNOWLEDGMENTS: The reported study was funded by RFBR, projects number 18-37-00459, 19-01-00364, 19-17-50094, 19-37-90022, 20-07-00652.