Серия «Математика»
2022. Т. 40. С. 63—77

Онлайн-доступ к журналу:
http://mathizv.isu.ru

ИЗВЕСТИЯ
Иркутского
государственного
университета

Research article

УДК 003.26
MSC 94A60
DOI https://doi.org/10.26516/1997-7670.2022.40.63

Обобщенная схема скрытого компактного хранения данных различных пользователей в общей открытой базе

В. А. Романьков[1]✉

[1] Омский государственный университет им. Ф. М. Достоевского, Омск, Российская Федерация
✉ romankov48@mail.ru

Аннотация. Базой данных называют набор структурированной информации, который обычно хранится в электронном виде в компьютерной системе и управляется системой управления базами данных (СУБД). Конфиденциальность, целостность и доступность являются основными требованиями безопасности базы данных. Данные в наиболее распространенных типах современных баз данных обычно хранятся в виде строк и столбцов формирующих таблицу, но также используются другие конфигурации. Использование публичных сетей и развитие информационных технологий (в том числе облачных) предъявляет новые повышенные требования к формированию баз данных. Первостепенным требованием становится защищенность баз данных от несанкционированных действий как самих пользователей, так и сторонних наблюдателей (потенциальных нарушителей). Криптографические средства защиты становятся важнейшим инструментом в обеспечении этого требования.

В настоящей работе на основе новых (введенных автором в недавней публикации) понятий обобщенных дискретных дифференцирования и интегрирования предлагается принципиально новая схема скрытого компактного хранения данных группы пользователей в общей открытой базе. Компонентами таблицы служат элементы кольца K, кодирующие данные. В работе предлагается использовать кольца вычетов. База не имеет подразделов, относящихся к данным индивидуальных пользователей. Соответствующая таблица является покомпонентной суммой индивидуальных таблиц, построенных определенным алгоритмом по данным каждого из пользователей. Любой из пользователей может извлечь из базы свои данные с помощью индивидуального ключа. Ключ выдается в момент регистрации пользователя в системе, когда создается и добавляется в базу таблица полученная на основе его данных. Ключ представляет из себя пару многочленов с коэффициентами из K с обратимыми старшими коэффициентами. Построение таблицы и алгоритмы извлечения из нее своих данных индивидуальными пользователями осуществляются эффективно. В то же время конкретный пользователь не имеет возможности

получить данные других пользователей. Сторонний наблюдатель (потенциальный нарушитель) не может получить никаких данных. Схема позволяет изменять и удалять данные без замены ключей. Свободный доступ к базе данных и многократное использование ключей являются основными достоинствами схемы.

Ключевые слова: дискретные дифференцирование и интегрирование, криптография, скрытое компактное хранение данных

Благодарности: Работа выполнена при финансовой поддержке РНФ, грант 22-21-00745.

Ссылка для цитирования: Романьков В.А. Обобщенная схема скрытого компактного хранения данных различных пользователей в общей открытой базе // Известия Иркутского государственного университета. Серия Математика. 2022. Т. 40. С. 63–77.
https://doi.org/10.26516/1997-7670. 2022.40.63

Research article

Generalized Scheme of Hidden Compact Storage of Data of Various Users in a Common Open Database

Vitaly A. Roman'kov[1]✉

[1] Dostoevsky Omsk State University, Omsk, Russian Federation
✉ romankov48@mail.ru

Abstract. A database is an organized collection of structured information, typically stored electronically in a computer system and usually controlled by a database management system (DBMS). Confidentiality, integrity and availability are the main requirements for database security. Data within the most common types of modern databases in operation is typically stored in rows and columns in a series of tables, but other configurations are also used. The use of public networks and the development of information technologies (including cloud ones) impose new increased requirements on the formation of databases. The paramount requirement is the security of databases from unauthorized actions of both the users themselves and third-party observers (potential violators). Cryptographic security tools are becoming an important tool to meet this requirement.

In this paper, based on new (introduced by the author in a recent publication) concepts of generalized discrete differentiation and integration, a fundamentally new scheme for hidden compact storage of user group data in a common open database is proposed. The components of the table are elements of the ring K that encode the data. The paper proposes to use residue rings. The database does not have subsections related to the data of individual users. The corresponding table is a component-by-component sum of individual tables built by a certain algorithm according to the data of each user. Any user can retrieve his data from the database using his own individual key. The construction of the table and the algorithms for extracting individual user data from it are carried out efficiently. A user gets the key at the time of his registration in the system, when his table (obtained on the basis of his data) is created and added to the database. The key has the form of two polynomials with coefficients from K with invertible leading coefficients. At the same time, a particular user does not have the opportunity to obtain the data of other users. An outside observer (potential intruder) cannot obtain any data.

The scheme allows changing and deleting data without replacing keys. Free access to the database and reuse of keys are the main advantages of the scheme.

Keywords: discrete differentiation and integration, cryptography, compact data storage

Acknowledgements: The work was supported by RSF, grant 22–21–00745.

For citation: Roman'kov V.A. Generalized Scheme of Hidden Compact Storage of Data of Various Users in a Common Open Database. *The Bulletin of Irkutsk State University. Series Mathematics*, 2022, vol. 40, pp. 63–77. (in Russian) https://doi.org/10.26516/1997-7670.2022.40.63

1. Введение

В современном мире существуют различные группы пользователей каких-либо систем. Типичным примером являются пациенты клиники. Клиника собирает и хранит информацию о своих пациентах в электронном виде. Информация часто является конфиденциальной, поэтому доступ к ней должен быть ограничен. Ограничение доступа может достигаться различными способами и средствами. В данной работе мы рассматриваем возможные криптографические средства. Аналогичная структура возникает, когда крупная организация использует криптосистему с открытым ключом, в которой формирует базу данных своих сотрудников. Различные способы создания такой системы и ее функционирования представлены в основополагающей статье Иво Десмедта [3].

Конечно, можно хранить данные каждого из сотрудников индивидуально в зашифрованном виде. В этом случае организация выбирает одну из систем шифрования, устанавливает ее на сервере и распределяет ключи расшифрования между сотрудниками, которые становятся таким образом пользователями системы. В дальнейшем каждый из них будет иметь возможность с помощью ключа расшифрования получать доступ к своим данным. Такая схема хранения данных очевидно неэффективна. Более рациональным способом является хранение данных в некоторой общей для группы пользователей открытой базе, из которой индивидуальные пользователи могут извлекать свои данные, опять же пользуясь некоторыми индивидуальными ключами. Важно предусмотреть возможность изменения или сокращения данных пользователей без изменения их индивидуальных ключей. При этом следует также позаботиться о компактности хранения данных, легкости их получения легитимными пользователями и в то же время защищенности сохраняемых данных от нелегитимных действий, скажем, подлога, подделки и подбора ключей. Эти требования стандартны для криптографии.

Общую информацию о данных, соответствующих криптографических задачах и некоторых базовых протоколах см. в монографиях [5;8].

Обзор практически используемых баз данных содержится в работах [4; 7].

В работе [2] автором был предложен принципиально новый способ скрытого компактного хранения данных различных пользователей в открытой базе, основанный на дискретных дифференцировании и интегрировании. Опишем этот способ в общих чертах

Пусть $A_1, \ldots, A_n$ — некоторая группа пользователей. Предполагается, что данные каждого из пользователей A_i закодированы элементом d_i кольца вычетов $\mathbb{Z}_m$, где модуль m соответствует этой группе пользователей. Модули различных групп могут как совпадать, так и отличаться друг от друга, это не имеет принципиального значения. Вместо $\mathbb{Z}_m$ можно использовать любое другое кольцо, допускающее кодировку данных.

В дальнейшем речь идет о выбранной группе пользователей. Для остальных групп пользователей (если они есть) процесс представления данных в базе точно такой же.

Все данные $D = \{d_1, \ldots, d_n\}$ преобразуются в содержание прямоугольной таблицы с элементами из $\mathbb{Z}_m$. Размеры таблицы объясняются ниже в разделе, описывающем указанные преобразования. При этом таблица не имеет разделителей (подтаблиц и т. п.) каким-нибудь образом соответствующих различным пользователям. Сначала на каждого пользователя A_i заполняется таблица $T(d_i)$, соответствующая его данным d_i. Затем все полученные индивидуальные таблицы $T(d_i)$ складываются поэлементно (согласно положению в таблице) в соответствии с операцией сложения кольца $\mathbb{Z}_m$, давая в итоге общую таблицу $T(D)$, которая служит базой хранения данных D. Построение индивидуальных таблиц $T(d_i)$ осуществляется с использованием известных дискретных операций дифференцирования и интегрирования последовательностей элементов кольца $\mathbb{Z}_m$. Секретность схемы обусловливается некоторыми трудноразрешимыми задачами связанными с этими понятиями.

Каждое из данных d_i может быть извлечено единообразным способом из построенной таблицы соответствующим пользователем A_i с использованием его индивидуального ключа.

Достоинствами метода, описанного в работе [2], являются: компактность таблицы, достаточно простой алгоритм ее построения, возможность изменения индивидуальных данных пользователей без изменения индивидуальных ключей, возможность удаления пользователей. Недостатком, на наш взгляд, является тот факт, что при задании индивидуальные ключи выглядят однообразно, притом в целом наблюдателю понятно, какие ключи используются, но неясно, какой ключ принадлежит какому из пользователей. При генерации ключей требуется выполнять возведение многочлена вида $x - 1 \in \mathbb{Z}_m[x]$, соответствующего стандартным дифференцированию и интегрированию, в большие степени. Для ускорения такого возведения приходится использовать соот-

ветствующие известные методы (относительно которых см., например, монографии [6; 11]).

Целью настоящей работы является построение на основе обобщений понятий дискретных дифференцирования и интегрирования схемы скрытого компактного хранения данных различных пользователей в открытой базе, которая является более защищенной, чем схема, построенная в [2]. В частности, она свободна от указанного выше недостатка. При этом сохраняются описанные выше достоинства, к которым добавляется достаточно быстрая генерация ключей простого и компактного вида, что позволяет значительно сократить время выполнения необходимых дифференцирований и интегрирований.

Структура статьи следующая. Раздел 2 посвящен определению и основным свойствам дискретных дифференцирования и интегрирования, а также их обобщений. Раздел 3 посвящен основной конструкции статьи — построению схемы скрытого компактного хранения данных индивидуальных пользователей в открытой общей базе на основе понятий обобщенных дискретных дифференцирования и интегрирования. Объясняется возможность извлечения индивидуальных данных из базы с помощью индивидуальных ключей. Также приводится анализ достоинств предлагаемой обобщенной схемы по сравнению с оригинальной схемой и ее секретности. В заключение приводится иллюстрирующий пример. Раздел 4 подытоживает достигнутые результаты.

2. Предварительные сведения: дискретные дифференцирование и интегрирование

В следующем подразделе приводятся оригинальные определения, использованные в [2].

2.1. Дискретные дифференцирование и интегрирование.

Понятие дискретного дифференцирования двусторонней последовательности элементов кольца целых чисел $\mathbb{Z}$ известно достаточно давно. Оно имеет ряд приложений (см., например, [12]), но до последнего времени практически не использовалось в серьезных исследованиях. Почти не рассматривалось и соответствующее ему дискретное интегрирование. Эти понятия применимы к любому кольцу K, а по сути они относятся к аддитивной группе K^+, так как используют только операцию сложения.

Дискретное дифференцирование определяется следующим образом. Пусть $\bar{a} = (\ldots, a_{-1}, a_0, a_1, \ldots) \in K^\infty$ – двусторонняя последовательность элементов кольца K. Дифференцирование $\delta : K^\infty \to K^\infty$ задает-

ся формулой

$$\delta(\bar{a}) = (..., -a_{-1} + a_0, -a_0 + a_1, -a_1 + a_2, ...).$$

Можно ограничить операцию дифференцирования на любой конечный интервал $\bar{a}(i,j), i < j$ вида $(a_i, \dots, a_j) \in K^{j-i}$. При этом оказывается не определенной j-я компонента значения дифференцирования. Аналогичным образом определяется дифференцирование для произвольной аддитивной абелевой группы A вместо K (т. е. по сути вместо K^+).

Заметим, что дискретное дифференцирование можно определить не только для кольца или аддитивной абелевой группы, но и для произвольной (в том числе некоммутативной) группы G с операцией умножения. Для произвольной последовательности $\bar{a} = (..., a_{-1}, a_0, a_1, \dots) \in G^\infty$ ее элементов дифференцирование определяется как отображение

$$\delta(\bar{a}) = (\dots, a_{-1}^{-1}a_0, a_0^{-1}a_1, a_1^{-1}a_2, \dots),$$

Считаем, что G^∞ — декартова степень группы G, на элементах которой определены операции покомпонентного умножения и взятия обратного элемента. Ее элементами являются двусторонние последовательности элементов группы G. Если G — абелева группа, то очевидно, что $\delta(\bar{a}^{-1}) = \delta(\bar{a})^{-1}$ и $\delta(\bar{a}\bar{b}) = \delta(\bar{a})\delta(\bar{b})$ для любых $\bar{a}, \bar{b} \in G^\infty$.

Рассмотрим декартово сплетение $\bar{G} = G\,Wr\,C_\infty$ группы G с бесконечной циклической группой $C_\infty = gp(c)$. Группа $\bar{G}$ есть полупрямое произведение базисной группы G^∞ с бесконечной циклической группой C_∞. Элемент c действует на элементы (последовательности) группы G^∞ левыми сдвигами. Для любой последовательности $\bar{a} \in G^\infty$ выполняется равенство

$$[\bar{a}, c] = \delta(\bar{a}).$$

В работе [10] показано, что для любого элемента $\bar{a} \in G^\infty$ существует элемент $\bar{b} \in G^\infty$ такой, что

$$[\bar{b}, c] = \bar{a}.$$

Любая пара таких элементов $\bar{b}$ отличается на константу (постоянную последовательность). Множество таких элементов естественно называть *первообразной* или *интегралом* от $\bar{a}$. Будем обозначать такое множество через $\iota(\bar{a})$. Элемент из $\iota(\bar{a})$ однозначно определяется любой своей фиксированной компонентой, которая может быть произвольной. Через $\iota_g(\bar{a})$ будем обозначать элемент из $\iota(\bar{a})$ со значением g в компоненте 1, т. е. $\iota_g(\bar{a})(1) = g$.

Понятия дискретного дифференцирования и дискретного интегрирования существенно использовались для получения основных результатов работ [2] и [10]. Отметим также, что в статье [9] было неявно доказано существование первообразной.

Перейдем к обобщениям обсуждаемых понятий, введенным в статье [1].

2.2. Обобщенные дискретные дифференцирование и интегрирование

Пусть K — произвольное кольцо. Наибольший интерес для наших приложений представляют конечные поля $\mathbb{F}_q, q = p^r$, порядка q характеристики p и кольца вычетов вида $\mathbb{Z}_m, m = pq$, где p и q — различные (большие) простые числа.

Для любого набора элементов $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_k) \in K^{k+1}$ определим дифференцирование $\delta_\alpha : K^\infty \to K^\infty$ следующим образом.

Пусть $\bar{a} = (\ldots, a_{-1}, a_0, a_1, \ldots) \in K^\infty$ – двусторонняя последовательность элементов кольца K. Тогда

$$\delta_\alpha(\bar{a}) = \bar{b} = (\ldots, b_1, b_0, b_1, \ldots),$$

где

$$b_i = \alpha_0 a_i + \alpha_1 a_1 + \ldots + \alpha_k a_{i+k}, i \in \mathbb{Z}.$$

Обычное дискретное дифференцирование представляет собой частный случай обобщенного, соответствующий набору $(-1, 1)$.

Ясно, что $\delta_\alpha : K^\infty \to K^\infty$ является аддитивной функцией, т. е. для любых $\bar{a}, \bar{b} \in K^\infty$ выполнены равенства $\delta(\bar{a} \pm \bar{b}) = \delta(\bar{a}) \pm \delta(\bar{b})$.

Следующий результат доказан в работе [1] (теорема 1) для случая конечного поля $\mathbb{F}_q$. При некоторых предположениях он справедлив для любого кольца K.

Теорема 1. *Пусть дифференцирование δ_α соответствует набору $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_k) \in K^{k+1}$, у которого элементы α_0 и α_k обратимы в кольце K. Тогда для любой последовательности $\bar{b} = (\ldots, b_{-1}, b_0, b_1, \ldots) \in K^\infty$ существует такая последовательность $\bar{a} = (\ldots, a_{-1}, a_0, a_1, \ldots) \in K^\infty$, что выполнено равенство*

$$\delta_\alpha(\bar{a}) = \bar{b}.$$

Другими словами, любая последовательность $\bar{b} \in K^\infty$ интегрируема. Последовательность $\bar{a}$ однозначно определяется набором компонент $(a_0, \ldots, a_{k-1})$, который может быть произвольным.

Доказательство. Значения $a_0, a_1, ..., a_{k-1}$ задаем произвольным образом. Элемент a_k определяем так, чтобы выполнялось равенство $b_0 = \sum_{i=0}^{k} \alpha_i a_i$. А именно:

$$a_k = \alpha_k^{-1} b_0 - \alpha_k^{-1} \sum_{i=0}^{k-1} \alpha_i a_i.$$

Далее последовательно вычисляем элементы $a_{k+j}, j = 1, 2, \ldots$, из соотношений $b_j = \sum_{i=0}^{k} \alpha_i a_{j+i}$. А именно:

$$a_{k+j} = \alpha_k^{-1} b_j - \alpha_k^{-1} \sum_{i=0}^{k-1} \alpha_i a_{j+i}.$$

Аналогично вычисляем a_{-1-j} для $j = 0, 1, \ldots$ из соотношений

$$a_{-1-j} = \alpha_0^{-1} b_{-1-j} - \alpha_0^{-1} \sum_{i=1}^{k} \alpha_i a_{-1-j+i}.$$

Утверждение теоремы проверяется непосредственно. □

Обозначим через $\mathrm{Ann}(\delta_\alpha)$ аннулятор дифференцирования δ_α в K^∞. *Первообразной* или *интегралом* $\iota_\alpha(\bar{b})$ последовательности $\bar{b}$ относительно набора α назовем множество всех последовательностей $\bar{a} \in K^\infty$ таких, что $\delta_\alpha(\bar{a}) = \bar{b}$. Ясно, что $\iota_\alpha(\bar{b}) = \bar{a} + \mathrm{Ann}(\delta_\alpha)$, где $\bar{a}$ – любая (частная) последовательность, для которой $\delta_\alpha(\bar{a}) = \bar{b}$.

С любым набором $\alpha = (\alpha_0, \ldots, \alpha_k)$ связан многочлен $f_\alpha(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k$ с коэффициентами из кольца K, и наоборот, любому такому многочлену соответствует набор коэффициентов α, по которому определяется дифференцирование δ_α. Многочлен $f_\alpha(x)$ назовем *определяющим для дифференцирования* δ_α или просто *определяющим*, если ясно, о каком дифференцировании идет речь. Мы пишем $\delta_\alpha = \delta_{f_\alpha}$. Аналогично обозначаем $\iota_\alpha = \iota_{f_\alpha}$, если по данному многочлену $f_\alpha(x)$ можно определить интегрирование (коэффициенты α_0 и α_k обратимы в K).

В работе [1] следующая теорема доказана также для случая конечного поля $\mathbb{F}_q$. Однако ее доказательство проходит для любого кольца K без каких-либо изменений или дополнительных условий.

Теорема 2. *([1], теорема 2). Пусть δ_α и δ_β – два дифференцирования K^∞, отвечающие наборам $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_k)$ и $\beta = (\beta_0, \beta_1, \ldots, \beta_l)$, соответственно. Тогда для любой последовательности $\bar{a} \in K^\infty$ справедливо равенство*

$$\delta_\beta(\delta_\alpha(\bar{a})) = \delta_\alpha(\delta_\beta(\bar{a})).$$

Другими словами, любые два обобщенных дифференцирования перестановочны между собой. Более того, суперпозиция этих дифференцирований, взятых в любом порядке, является дифференцированием, соответствующим произведению определяющих многочленов $f_\alpha(x)$ и $f_\beta(x)$.

Доказательство проводится прямым вычислением (см. [1]).

Интегрирования между собой и интегрирования с дифференцированиями в общем случае не перестановочны.

Замечание 1. Дифференцировать и интегрировать можно также односторонние правонаправленные и конечные последовательности. Во втором случае в последовательности должно быть не меньше элементов, чем степень соответствующего многочлена плюс 1. При интегрировании излишне требование обратимости коэффициента α_0 (свободного члена в соответствующем определяющем многочлене). Результатом

дифференцирования или интегрирования односторонней правонаправленной последовательности и интегрирования конечной последовательности будет последовательность такого же вида.

При дифференцировании конечной последовательности получается последовательность меньшей длины на величину равную степени определяющего многочлена.

3. Обобщенная схема секретного компактного хранения данных

Итак, имеется группа пользователей $A_1, \ldots, A_n$ некоторой криптографической системы, установленной Алисой. Предполагается, что данные каждого из пользователей A_i закодированы элементом d_i кольца вычетов $\mathbb{Z}_m$.

В дальнейшем для передачи индивидуальных ключей и размещения таблицы $T(D)$ Алиса использует одну из двух следующих моделей.

1. *Модель защищенного канала связи.* Коммуникации между Алисой и пользователями системы осуществляются по защищенной сети. В этой модели пользователи могут видеть только передаваемые сообщения и файлы, размещенные внутри сети. Внешние наблюдатели не имеют доступа к сети.

2. *Модель открытого канала связи.* Коммуникации между Алисой и пользователями осуществляются по открытой сети. Все пользователи, а также внешние наблюдатели могут получать все передаваемые сообщения и читать все созданные файлы этой сети.

Алиса создает систему шифрования, в которой участники процесса $A_1, A_2, \ldots, A_n$ регистрируются в качестве пользователей. Алиса создает сайт, в котором размещает таблицу $T(D)$. Затем Алиса передает секретным образом каждому пользователю A_i индивидуальный ключ $K_i = (f_i(x), g_i(y))$. Знание ключа позволяет пользователю A_i вычислить свои индивидуальные данные d_i из размещенной таблицы $T(D)$. Способ такого вычисления объясняется ниже.

3.1. Описание схемы

Алиса для организации скрытого компактного хранения данных $D = (d_1, \ldots, d_n)$ производит следующие действия.

– Сначала Алиса выбирает две группы многочленов: $f_1(x), \ldots, f_n(x)$ и $g_1(y), \ldots, g_n(y)$ таких, что степени многочленов $f_i(x)$ строго возрастают, а многочленов $g_j(y)$ строго убывают. При этом каждый из многочленов $f_i(x), i \leq n-1$, делит следующий многочлен $f_{i+1}(x)$, а каждый многочлен $g_j(y), j \geq 2$, делит предыдущий многочлен

$g_{j-1}(y)$. Мы также считаем, что частные $u_i(x) = f_{i+1}(x)/f_i(x), i \geq 2$, равно как и $v_j(y) = g_j(y)/g_{j+1}(y), j \leq n-1$, имеют нулевые суммы коэффициентов. Таким образом

$$f_i(x) = u_{i-1}(x) \dots u_1(x) f_1(x),\ g_j(y) = v_j(y) \dots v_{n-1}(y) g_n(y). \quad (3.1)$$

– Далее Алиса строит прямоугольную таблицу ширины t_1 и высоты t_2. Строки занумерованы от 0 до t_2-1 снизу вверх, столбцы от 0 до t_1-1 слева направо. Необходимым условием для вычисления интегралов при заполнении таблицы является выполнение неравенств $t_1 \geq max\{degree(g_j(y)) : j = 1, 2, \dots, n\}$, $t_2 \geq max\{degree(f_i(x)) : i = 1, 2, \dots, n\}$.

Затем Алиса заполняет индивидуальные таблицы $T(d_i)$ для каждого пользователя A_i, $i = 1, \dots, n$.

– Для каждого i заполняется нулевая строка таблицы $T(d_i)$ значениями, которые получаются последовательным вычислением интегралов ι_{g_i} в соответствии с представлением 3.1 от начального значения $\tilde{\tilde{d}}_i$, где $\tilde{\tilde{d}}_i$ обозначает постоянную последовательность с элементами d_i. Более точно: сначала вычисляется интеграл $\iota_{v_i}(\tilde{\tilde{d}}_i)$, затем вычисляется интеграл $\iota_{v_{i+1}}(\iota_{v_i}(\tilde{\tilde{d}}_i))$ и так далее до вычисления интегралов $\iota_{v_{n-1}}$ и ι_{g_n} от полученных на предыдущем шаге последовательностей каждый раз со значением $d_{i,0} = d_i$ в начальной клетке. Выбор других начальных констант при интегрировании может быть произвольным. Получается строка $R_{i,0} = (d_{i,0}, \dots, d_{i,t_1-1})$.
– Далее столбцы таблицы $T(d_i)$ дополняются постоянными значениями, равными соответствующему значению в строке $R_{i,0}$, т. е. все компоненты столбца с номером j становятся равными $d_{i,j}$. Затем для заполнения этого столбца, как и выше для строки $R_{i,0}$, последовательно вычисляются интегралы $\iota_{u_{i-1}}, \dots, \iota_{u_1}, \iota_{f_1}$ каждый раз со значением $d_{i,j}$ в начальной клетке. Выбор других начальных констант при интегрировании может быть произвольным. Полученный столбец обозначим через $B_{i,j}$.

Далее все полученные таблицы $T(d_i)$ складываются покомпонентно согласно операции сложения в $\mathbb{Z}_m$, давая в результате итоговую таблицу данных $T(D)$. В частности в угловой клетке таблицы $T(D)$ стоит сумма $\sum_{i=1}^{n} d_i$ закодированных данных всех пользователей.

Способ вычисления данных d_i из таблицы $T(D)$ пользователем A_i с помощью ключа $K_i = (f_i(x), g_i(y)$ выводится из следующего результата.

Теорема 3. *Если пользователь $A_i, i \in \{1, 2, \dots, n\}$, применит к каждому столбцу $B_j(D)$ таблицы $T(D)$ дифференцирование δ_{f_i}, а затем для нулевой строки полученной таблицы вычислит дифференцирование δ_{g_i}, то в нижнем левом углу он получит свои закодированные данные d_i.*

Доказательство. Каждый столбец $B_j(D)$ таблицы $T(D)$ есть сумма столбцов $B_{l,j}$, $l = 1, \ldots, n$. Дифференцирование аддитивно, поэтому посмотрим, как действует δ_{f_i} на каждый из столбцов $B_{l,j}$. Нас интересует только значение результата в нулевой строке.

- Пусть $l = i$. Очевидно, что рассматриваемое значение равно $d_{i,j}$, т. е. совпадает с соответствующим значением в строке $R_{i,0}$.
- Если $l < j$, то дифференцирование δ_{f_i} есть суперпозиция дифференцирования δ_{f_l}, после выполнения которого получается столбец постоянных значений, и дифференцирования, для определяющего многочлена которого сумма коэффициентов равна 0. Второе дифференцирование обнуляет все значения данного столбца, в частности, оно имеет значение 0 в нулевой.
- Если $l > i$, то дифференцирование δ_{f_i} приводит к результату, полученному после интегрирования столбца с постоянным значением $d_{l,j}$ последовательностью интегрирований $\iota_{l-1}, \ldots, \iota_i$. Согласно сделанным предположениям это значение равно $d_{l,j}$.

После приведенных вычислений в строке $R_{i,0}$ остались данные пользователей $A_i, \ldots, A_n,$, совпадающие с соответствующими их начальными данными в этой строке.

Затем пользователь A_i применяет дифференцирование δ_{g_i} к полученной нулевой строке. Строка есть сумма строк, соответствующих пользователям $A_i, \ldots, A_n$. Строка, соответствующая A_l при $l > i$, дает нулевой результат по рассуждению, аналогично доказанному выше для столбцов. Дифференцирование строки соответствующей A_i имеет постоянное значение d_i во всех клетках, для которых его можно вычислить. Начальная клетка входит в это множество. □

В таблице $T(D)$ можно заменять данные пользователей без изменения их индивидуальных ключей. При замене d_i на новое значение d_i' Алисе необходимо произвести покомпонентное вычитание $T(D) - T(d_i)$, вычислить точно так же, как и раньше, таблицу $T(d_i')$ и сложить ее покомпонентно с таблицей $T(D) - T(d_i)$. Также можно удалить из системы какого-либо пользователя A_i с заменой $T(D)$ на $T(D) - T(d_i)$.

3.2. Эффективность выполняемых алгоритмов и защищенность данных

При использовании определяющих многочленов $f_i(x)$ и $g_j(y)$ с малыми множествами ненулевых коэффициентов сокращается время выполнения необходимых дифференцирований и интегрирований по сравнению со схемой из статьи [1]. В той схеме приходилось вычислять и использовать большие степени стандартных определяющих многочленов $x - 1$ и $y - 1$, для чего требовалось пользоваться известными ускоренными методами возведения в степень. В предлагаемой схеме

можно, например, использовать многочлены вида $x^k - 1$, у которых k имеет много делителей. Если, $k = k_1 \dots k_r$, то $x^k - 1$ делится на многочлен $x^{k_1 \dots k_{r-1}} - 1$, тот в свою очередь делится на $x^{k_1 \dots k_{r-2}} - 1$ и т. д.

Вычисление данных пользователей алгоритмом подбора ключей $K_i = (f_i(x), g_i(y))$ можно пытаться осуществить следующим образом. Размеры таблицы $T(D)$ ограничивают степени многочленов $f_i(x)$ и $g_i(y)$. А именно: степени многочленов $f_i(x)$ не превосходят высоты таблицы t_2, а степени многочленов $g_i(y)$ — ширины таблицы t_1. Если взять пару многочленов с этим условием $(f(x), g(y))$ (старшие коэффициенты этих многочленов должны быть обратимы), затем применить к каждому столбцу таблицы $T(D)$ дифференцирование δ_f, после чего выполнить для нулевой строки дифференцирование δ_g (операции из теоремы 3), в нижнем левом углу будет стоять вычет d. По нему восстанавливается некоторый текст. Если получился осмысленный текст с описанием данных пользователя A_i, значит, подобран ключ $(f_i(x), g_i(y))$. Такой подбор практически осуществим при сравнительно небольших параметрах m, t_1, t_2.

Если удастся вычленить из $T(D)$ таблицу $T(d_i)$, то возникнет проблема вычисления ключа $K_i = (f_i(x), g_i(y))$ для получения в дальнейшем измененных данных d_i. Аналогично работе [1] можно показать, что подбор элемента $f_i(x)$ такого ключа возможен только при решении системы, состоящей в общем случае из t_2 линейных уравнений. После этого для вычисления $g_i(y)$ потребуется решить систему из t_1 линейных уравнений. При этом не появится существенной информации о других ключах $K_j = (f_j(x), g_j(y))$.

Возможность иных более продуктивных подходов к доказательству защищенности или уязвимости предлагаемой схемы остается открытой проблемой.

Для иллюстрации предлагаемой схемы приведем простейший пример. Все обозначения соответствуют введенным выше.

Пример 1. Предположим, что группа состоит из трех пользователей: A_1, A_2, A_3. Рассматриваемые таблицы имеют оазмер 4×4. Определяющими будут многочлены $f_1(x) = x + 1, f_2(x) = x^2 - 1 = (x - 1)(x + 1), f_3(x) = x^3 - x^2 - x + 1 = (x - 1)(x - 1)(x + 1); g_1(y) = y^3 - y^2 - y + 1 = (y - 1)(y - 1)(y + 1), g_2(y) = y^2 - 1 = (y - 1)(y + 1), g_3(y) = y - 1$. Заметим, что разложения на множители в указанном порядке необходимы для порядка выполнения интегрирований, осуществляемых Алисой.

Мы опускаем достаточно простые вычисления, приводя только итоговые индивидуальные таблицы $T(d_i)$, $i = 1, 2, 3$.

$$\begin{pmatrix} 2d_1 & 0 & 2d_1 & 0 \\ 2d_1 & 0 & 2d_1 & 0 \\ 0 & 0 & 0 & 0 \\ d_1 & 0 & d_1 & 0 \end{pmatrix}, \begin{pmatrix} 2d_1 & 0 & 2d_1 & 0 \\ 2d_1 & 0 & 2d_1 & 0 \\ 0 & 0 & 0 & 0 \\ d_1 & 0 & d_1 & 0 \end{pmatrix}, \begin{pmatrix} 2d_1 & 0 & 2d_1 & 0 \\ 2d_1 & 0 & 2d_1 & 0 \\ 0 & 0 & 0 & 0 \\ d_1 & 0 & d_1 & 0 \end{pmatrix}.$$

Выбирая кольцо $\mathbb{Z}_m$ и придавая конкретные значения вычетам $d_i \in \mathbb{Z}_m$, $i = 1, 2, 3$, мы получим числовые индивидуальные таблицы пользователей. После их покомпонентного сложения получим таблицу $T(D)$.

4. Заключение

В работе предложена новая схема скрытого компактного хранения данных группы пользователей в открытой базе, основанная на обобщениях понятий дискретных дифференцирования и интегрирования. Каждый из пользователей может извлечь из базы свои данные с помощью индивидуального ключа. При этом ни он, ни тем более сторонний наблюдатель, не способны получить какую-либо существенную информацию о данных других пользователей. Схема позволяет изменять данные пользователей без замены ключей. Создание базы данных и последующие ее изменения выполняются эффективно. Извлечение своих данных индивидуальным пользователем также осуществляется эффективно. Этому способствует правильный выбор многочленов, определяющих выполняемые дифференцирования и интегрирования. В отличие от ранее предложенной автором схемы, основанной на стандартных дискретных операциях дифференцирования и интегрирования, предлагаемая схема более защищенная, а ее алгоритмы более эффективны. Они, в частности, не используют возведение многочленов в большие степени.

Список источников

1. Волошин С. К., Романьков В. А. Обобщенные дискретные операции дифференцирования и интегрирования // Вестник Омского университета. 2021. Т. 26, № 4. С. 4–8. https://doi.org/10.24147/1812-3996.2021.26(4). С. 4–8.
2. Романьков В. А. О скрытом компактном способе хранения данных // Прикладная дискретная математика. Приложение. 2020. № 13. С. 56–59. https://doi.org/10.17223/2226308X/13/17.
3. Desmedt Y. Society and group oriented cryptography: A new concept // Conference on the Theory and Application of Cryptographic Techniques. Berlin, Heidelberg : Springer, 1987. P. 120–127.
4. Survey on securing data storage in the cloud / C.-T. Huang, L. Huang, Z. Qin, C.-C. J. Kuo, H. Yuan, L. Zhou, V. Varadharadjan, C.-C. J. Kuo // APSIPA Transactions on Signal and Information Processing. 2014. Vol. 3. P. 1–17. https://doi.org/10.1017/ATSIP.2014.6.
5. Katz J., Lindell Y. Introduction to Modern Cryptography. Boca Raton, London, New York, Washington D.C. : CRC Press, 2007. 498 p.
6. Knuth D. E. The Art of Computer Programming. New York : Addison-Wesley Professional, 2011. 912 p.

7. A survey on data storage and placement methodologies for Cloud-Big Data ecosystem / S. Mazumdar, D. Seybold, K. Kritikos, Y. Verginadis // J. Big Data. 2019. Vol. 6. P. 6–37. https://doi.org/10.1186/s40537-019-0178-3.
8. Menezes A. J., Vanstone S. A., Oorschot P. C. van. Handbook of Applied Cryptography. Boca Rapton : CRC Press, 1996. 816 p.
9. Neumann P. M. On the structure of standard wreath products of groups // Math. Z. 1964. Vol. 84. P. 343–373. https:/doi.org/10.1007/BF01109904.
10. Roman'kov V. A. Embedding theorems for solvable groups // Proc. Amer. Math. Soc. 2021. Vol. 149, N 10. P. 4133–4143. https://doi.org/10.1090/proc/15562.
11. Smart N. Cryptography: An Introduction. New York : McGraw-Hill College, 2004. 433 p.
12. Thammattor A. Normal Limit of the Binomial via the Discrete Derivative // The College Mathematics Journal. 2018. Vol. 49, N 3. P. 216–217. https://doi.org./10.1080/07468342.2018.1440872.

References

1. Voloshin S.K., Roman'kov V.A. Obobshenniye discretniye operacii differencirovaniya i integrirovaniya [Generalized discrete operations of differentiation and integration]. *Herald of Omsk University*, 2021, vol. 26, no. 4, pp. 4–8. https://doi.org/10.24147/1812-3996.2021.26(4).4–8. (in Russian)
2. Roman'kov V.A. O skrytom kompactnom sposobe khraneniya dannih [About the hidden compact way to store data]. *Applied discrete mathematics. Applications*, 2020, no. 13, pp. 56–59. https://doi.org/10.17223/2226308X/13/17. (in Russian)
3. Desmedt Y. Society and group oriented cryptography: A new concept. *Conference on the Theory and Application of Cryptographic Techniques*. Berlin, Heidelberg, Springer, 1987, pp. 120–127.
4. Huang C.-T., Huang L., Qin Z., Kuo C.-C.J., Yuan H., Zhou L., Varadharadjan V., and Kuo C.-C.J. Survey on securing data storage in the cloud. *APSIPA Transactions on Signal and Information Processing*, 2014, vol. 3, pp. 1–17. https://doi.org/10.1017/ATSIP.2014.6.
5. Katz J., Lindell Y. *Introduction to Modern Cryptography*. Boca Raton, London, New York, Washington D.C., CRC Press, 2007, 498 p.
6. Knuth D.E. *The Art of Computer Programming*. New York, Addison-Wesley Professional Publ., 2011, 912 p.
7. Mazumdar S., Seybold D., Kritikos K., and Verginadis Y. A survey on data storage and placement methodologies for Cloud-Big Data ecosystem. *J Big Data*, 2019, vol. 6, pp. 6–37. https://doi.org/10.1186/s40537-019-0178-3.
8. Menezes A.J., Vanstone S.A., and Oorschot P.C. van. *Handbook of Applied Cryptography*. Boca Raton, CRC Press, 1996, 816 p.
9. Neumann P.M. On the structure of standard wreath products of groups. *Math. Z.*, 1964, vol. 84, pp. 343–373. https://doi.org.//10.1007/BF01109904.
10. Roman'kov V.A. Embedding theorems for solvable groups. *Proc. Amer. Math. Soc.*, 2021, vol. 149, no. 10, pp. 4133–4143. https://doi.org/10.1090/proc/15562.
11. Smart N. *Cryptography: An Introduction*. New York, McGraw-Hill College Publ., 2004, 433 p.
12. Thammattor A. Normal Limit of the Binomial via the Discrete Derivative. *The College Mathematics Journal*, 2018, vol. 49, no. 3, pp. 216–217. https://doi.org./10.1080/07468342.2018.1440872.

Об авторах

Романьков Виталий Анатольевич, д-р физ.-мат. наук, проф., Омский государственный университет им. Ф. М. Достоевского, Российская Федерация, 644077, г. Омск, romankov48@mail.ru, https://orcid.org/0000-0001-8713-7170

About the authors

Vitaly Roman'kov, Dr. Sci. (Phys.–Math.), Prof., Dostoevsky Omsk State University, Omsk, 644077, Russian Federation, romankov48@mail.ru, https://orcid.org/0000-0001-8713-7170

Поступила в редакцию / Received 21.01.2022
Поступила после рецензирования / Revised 10.03.2022
Принята к публикации / Accepted 14.03.2022