ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 512.54; 003.26 DOI 10.17223/20710410/61/1

ДИСКРЕТНЫЕ ДИФФЕРЕНЦИРОВАНИЯ И ИНТЕГРИРОВАНИЯ И ИХ ВОЗМОЖНЫЕ ПРИЛОЖЕНИЯ К АЛГЕБРЕ И КРИПТОГРАФИИ[1]

С. К. Волошин*, В. А. Романьков**

*Омский государственный университет им. Ф. М. Достоевского, г. Омск, Россия
** Институт математики им. С. Л. Соболева СО РАН, г. Омск, Россия

E-mail: savva.voloshin@gmail.com romankov48@mail.ru

Определяются обобщённые операции дискретных дифференцирования и интегрирования. Приводятся некоторые их свойства. Даётся краткий обзор полученных с использованием этих понятий результатов в алгебре и криптографии. Предлагается новая схема зашифрования сообщения на основе этих операций. Показывается, как их можно использовать для аутентификации и распределения ключа.

Ключевые слова: *дискретные дифференцирование и интегрирование, схема зашифрования, аутентификация, распределение ключа.*

DISCRETE DIFFERENTIATIONS AND INTEGRATIONS AND THEIR POSSIBLE APPLICATIONS TO ALGEBRA AND CRYPTOGRAPHY

S. K. Voloshin*, V. A. Roman'kov**

*Dostoevsky Omsk State University, Omsk, Russia
**Sobolev Institute of Mathematics SB RAS, Omsk, Russia

Generalized operations of discrete differentiation and integration are defined. Some of their properties are given. A brief review of the results obtained earlier with the use of these concepts in algebra and cryptography is given. A new message encryption scheme based on these operations is proposed. We also show how they can be used for authentication and key distribution.

Keywords: *discrete differentiations and integrations, encryption scheme, autentification, key distribution.*

Введение

В настоящее время ведётся интенсивный поиск новых инструментов для разработки криптографических схем и протоколов, в том числе устойчивых к атакам с помощью квантовых компьютеров. В данной работе в качестве такого инструмента предлагаются обобщённые дискретные дифференцирования и интегрирования. Впервые эти

[1]Работа второго автора выполнена в рамках госзадания ИМ СО РАН, проект FWNF–2022–0003.

операции определены авторами в [1] и использованы вторым автором в [2]. До этого было известно только обычное дискретное дифференцирование, применённое в работах [3, 4], в которых впервые доказано существование обычного дискретного интегрирования. Указаны некоторые возможности такого использования. Отмечено, что данные операции находят применение в алгебре.

Далее используются следующие обозначения: $\mathbb{Z}$ — кольцо целых чисел; $\mathbb{Z}_n$ — кольцо вычетов по модулю n; $\mathbb{F}_q$ — конечное поле порядка q; $\mathrm{GL}_s(K)$ — группа обратимых $k\times k$-матриц над кольцом K; $\mathrm{M}_k(K)$ — кольцо $k\times k$-матриц над кольцом K.

1. Определение и основные свойства обобщённых дискретных дифференцирований и интегрирований

Пусть K — произвольное коммутативное кольцо с единицей. Наибольший интерес для наших приложений представляют конечные поля $\mathbb{F}_q$, $q=p^r$, порядка q характеристики p и кольца вычетов вида $\mathbb{Z}_n$, $n=pq$, где p и q — различные (большие) простые числа. Операции обобщённых дискретных дифференцирований и интегрирований определяются на множестве бесконечных двусторонних последовательностей $\bar a=(\ldots,a_{-1},a_0,a_1,\ldots)$ элементов K. Они индуцируют соответствующие операции на односторонних бесконечных последовательностях и на конечных наборах элементов K. Сложение и умножение таких последовательностей задаются покомпонентно.

В общем случае дискретное дифференцирование δ_α определено набором элементов $\alpha=(\alpha_0,\alpha_1,\ldots,\alpha_k)\in K^{k+1}$. По определению

$$\delta_\alpha(\bar a)=(\ldots,b_{-1},b_0,b_1,b_2,\ldots),\ \text{где } b_i=\alpha_0a_i+\alpha_1a_{i+1}+\ldots+\alpha_ka_{i+k},\ i\in\mathbb{Z}. \qquad (1)$$

Обычное дискретное дифференцирование определяется набором $\alpha=(-1,1)$ или, проще говоря, формулой $b_i=a_{i+1}-a_i$, $i\in\mathbb{Z}$. Если понятно из контекста, о каком наборе параметров α идёт речь, или указывается свойство, справедливое для всех параметров, пишем δ, не указывая набор.

Ясно, что δ является аддитивной функцией, то есть для любых $\bar a,\bar b\in K^\infty$ выполнены равенства $\delta(\bar a\pm\bar b)=\delta(\bar a)\pm\delta(\bar b)$.

С любым набором $\alpha=(\alpha_0,\ldots,\alpha_k)$ связан многочлен $f_\alpha(x)=\alpha_0+\alpha_1x+\ldots+\alpha_kx^k$ с коэффициентами из кольца K, и наоборот, любому такому многочлену соответствует набор коэффициентов α, по которому определяется дифференцирование δ_α. Многочлен $f_\alpha(x)$ назовём *определяющим для дифференцирования* δ_α или просто *определяющим*, если ясно, о каком дифференцировании идет речь.

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. Непосредственно доказывается, что суперпозиция этих дифференцирований, взятых в любом порядке, является дифференцированием, соответствующим произведению определяющих многочленов $f_\alpha(x)$ и $g_\beta(x)$. Отсюда следует, что 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 обобщённых дифференцирования перестановочны между собой. В [1] этот результат отмечен для частного случая конечного поля $\mathbb{F}_q$.

Следующий результат доказан в [1, теорема 1] также для случая конечного поля $\mathbb{F}_q$. Он справедлив для любого коммутативного кольца K с единицей.

Теорема 1 [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 $(a_0, \ldots, a_{k-1})$, значения которых можно задать произвольно.

Доказательство. Значения $a_0, a_1, \ldots, a_{k-1}$ задаём произвольным образом. Элемент a_k определяем так, чтобы выполнялось равенство $b_0 = \sum\limits_{i=0}^{k} \alpha_i a_i$, 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 $b_j = \sum\limits_{i=0}^{k} \alpha_i a_{j+i}$:

$$a_{k+j} = \alpha_k^{-1} b_j - \alpha_k^{-1} \sum_{i=0}^{k-1} \alpha_i a_{j+i}. \tag{2}$$

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

$$a_{-1-j} = \alpha_0^{-1} b_{-1-j} - \alpha_0^{-1} \sum_{i=1}^{k} \alpha_i a_{-1-j+i}. \tag{3}$$

Утверждение теоремы проверяется непосредственно. ■

Первообразной или *интегралом* $\iota_\alpha(\bar{b})$ последовательности $\bar{b}$ относительно набора α назовём множество всех последовательностей $\bar{a} \in K^\infty$, таких, что $\delta_\alpha(\bar{a}) = \bar{b}$.

Обозначим через $\mathrm{Ann}(\delta_\alpha)$ аннулятор дифференцирования δ_α в K^∞. Ясно, что $\iota_\alpha(\bar{b}) = \bar{a} + \mathrm{Ann}(\delta_\alpha)$, где $\bar{a}$ — любая (частная) последовательность, для которой $\delta_\alpha(\bar{a}) = \bar{b}$. Такая частная последовательность задаётся формулами (2) и (3).

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). Конкретный элемент из ι_α однозначно определяется набором $\bar{a}_k = (a_0, a_1, \ldots, a_{k-1}) \in K^{k+1}$, который будем называть набором *констант*. Соответствующее значение по формулам (2) и (3) обозначаем $\iota_{\alpha,\bar{a}_k}$ и называем *определённым интегралом*, отвечающим выбору $\bar{a}_k$. Для любого $\bar{a}_k$ и произвольного набора α, по которому определяется интегрирование, выполнено равенство

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

Поэтому мы будем также использовать формулу

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

Другими словами, дифференцирование δ_α определяет правый обратный элемент к интегрированию ι_α. Заметим, что формула

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

выполнена только в том случае, когда $\bar{a}_k = \bar{b}_k$, то есть когда набор констант $\bar{a}_k$ совпадает с начальным набором $\bar{b}_k$ последовательности $\bar{b}$.

Замечание 1. Дифференцирование (1) индуцирует отображение любого бесконечного правостороннего интервала $\bar{a}_r(i) = (a_i, a_{i+1}, \ldots)$, $i \in \mathbb{Z}$, результатом которого является правосторонний интервал $\bar{b}_r(i) = (b_i, b_{i+1}, \ldots)$. Более того, областью определения может быть любой конечный интервал $(a_i, a_{i+1}, \ldots, a_{i+k+t})$, $t = 0, 1, 2, \ldots$, длины не меньше чем $k+1$, где k — степень определяющего многочлена. Результатом будет интервал $b_i, b_{i+1}, \ldots, b_{i+t}$ меньшей на величину k длины. Эти отображения будем также называть *дифференцированиями*. Для них выполнено утверждение о перестановочности дифференцирований. В дальнейшем мы не употребляем специальные обозначения для различных типов интервалов.

Интегрирования индуцируют отображения (*интегрирования*) как бесконечных правосторонних последовательностей, так и конечных наборов длины не меньше $k+1$. Считаем, что в этом случае набор начальных констант индексирован как крайний левый набор данной последовательности. Далее рассматриваются только правые интегрирования, по определению не вычисляющие элементы с меньшими индексами, чем у данной последовательности. В этом случае условие обратимости накладывается только на старший коэффициент α_k определяющего многочлена. Результатом такого отображения является соответственно бесконечная правосторонняя последовательность или конечный интервал длины на k больше интегрируемого.

Дифференцирования и интегрирования на нитях и их комбинации с линейными преобразованиями

Пусть по-прежнему K обозначает коммутативное кольцо с единицей. Допустим, задано s последовательностей (нитей) $a_1, \ldots, a_s$ одинаковых типов и равных соответствующих параметров, то есть это либо двусторонние бесконечные последовательности, либо односторонние правонаправленные бесконечные последовательности, либо наборы одинаковой длины. Дифференцирование δ_α и интегрирование i_α действуют одновременно на каждую из этих последовательностей. Считаем, что для интегрирований можно брать различные наборы констант. Пусть φ обозначает линейное преобразование нитей. Его можно задать матрицей A_φ. Далее рассматриваем только невырожденные преобразования, то есть $A_\varphi \in \mathrm{GL}_s(K)$. Очевидно, что операции дифференцирования и интегрирования перестановочны с линейными преобразованиями нитей. Суперпозицию дифференцирования и линейного преобразования обозначаем через $\delta_{\alpha,\varphi}$ и называем *скрученным дифференцированием*. Аналогично вводится понятие *скрученного интегрирования* $\iota_{\alpha,\varphi}$. Имеет место формула

$$\delta_{\alpha,\varphi^{-1}}(\iota_{\alpha,\varphi}(\bar{b})) = \bar{b}.$$

2. Возможные применения дискретных дифференцирований и интегрирований в алгебре

Понятия дискретных дифференцирования и интегрирования можно определить на произвольной группе G, в том числе некоммутативной. Они существенно использовались для получения основных результатов работы [4]. Отметим также, что в [5] неявно доказано существование первообразной.

При этом используется мультипликативная запись операции в группе G. Определяющий многочлен $f_\alpha(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k$ берётся с коэффициентами из кольца целых чисел $\mathbb{Z}$. Дифференцирование определяется формулой

$$\delta_\alpha(\bar{a}) = (\ldots, b_{-1}, b_0, b_1, b_2, \ldots), \quad b_i = a_i^{\alpha_0} a_{i+1}^{\alpha_1} \cdots a_{i+k}^{\alpha_k}, \quad i \in \mathbb{Z}.$$

Обычное (не обобщённое) дискретное дифференцирование определяется, как и в случае кольца, набором $\alpha = (-1, 1)$ или формулой $b_i = a_i^{-1} a_{i+1}$, $i \in \mathbb{Z}$. Интегрирование определено для любого определяющего многочлена с обратимыми коэффициентами α_0 и α_k формулой

$$\iota_\alpha(\bar{b}) = (\ldots, a_{-1}, a_0, a_1, a_2, \ldots),$$

где $\bar{a}_k = (a_0, a_1, \ldots, a_{k-1}) \in G^k$ — произвольный набор констант;

$$a_{k+j} = (a_{k+j-1}^{-\alpha_{k-1}} a_{k+j-2}^{-\alpha_{k-2}} \ldots a_{k+j}^{-\alpha_0} b_{k+j})^{\alpha_k^{-1}}, \quad j \in \mathbb{N} \cup \{0\};$$
$$a_{-j} = (a_{-j+1}^{\alpha_1} a_{-j+2}^{\alpha_2} \ldots a_{-j+k}^{\alpha_k} b_{-j})^{\alpha_0^{-1}}, \quad j \in \mathbb{N}.$$

3. Возможные применения дискретных дифференцирований и интегрирований в криптографии

В работах [6–13] и ряде других публикаций (см. библиографию в [9]) представлены методы криптографического анализа, показавшие уязвимость всех основных схем алгебраической криптографии. Поэтому актуален поиск новых криптографических инструментов для создания таких схем. В этом направлении ведётся и настоящее исследование.

На основе новых понятий обобщённых дискретных дифференцирования и интегрирования в работах [2, 3] предложена новая схема скрытого компактного хранения данных группы пользователей в общей открытой базе в виде таблицы. Компонентами таблицы служат элементы коммутативного кольца с единицей K, кодирующие данные. База не имеет подразделов, относящихся к данным индивидуальных пользователей. Соответствующая таблица является покомпонентной суммой индивидуальных таблиц, построенных определённым алгоритмом. Каждый из пользователей может извлечь из базы свои данные с помощью индивидуального ключа. Ключ выдаётся в момент регистрации пользователя в системе, когда создаётся таблица, полученная на основе его данных. Ключ представляет собой пару многочленов с коэффициентами из K с обратимыми старшими коэффициентами. Построение таблицы и алгоритмы извлечения из неё своих данных индивидуальными пользователями осуществляются эффективно. В то же время конкретный пользователь не имеет возможности получить данные других пользователей. Потенциальный нарушитель не может получить никаких данных. Схема позволяет изменять и удалять данные без замены ключей. Предполагается свободный доступ к базе данных. Возможно многократное использование ключей, что является основным достоинством схемы.

3.1. Передача зашифрованного сообщения

Алиса хочет передать сообщение, представленное конечной последовательностью s наборов $\bar{A} = (\bar{a}_1, \ldots, \bar{a}_s)$, где $\bar{a}_j = (a_{j,0}, \ldots, a_{j,l})$, фиксированной длины $l+1$ с элементами из коммутативного кольца с единицей K.

Перемешивание нитей проводится Алисой и Бобом и осуществляется умножением на матрицы $P_A, P_B \in \mathrm{GL}(K)$ соответственно. На последующих шагах корреспонденты используют обратные преобразования с матрицами P_A^{-1}, P_B^{-1} соответственно. Матрицы должны быть перестановочны между собой. Поэтому корреспонденты сначала договариваются о множестве M попарно перестановочных матриц из $\mathrm{GL}_s(K)$. Самым распространённым способом служит выбор матрицы T и определение в качестве M множества значений всех многочленов вида $u(x) \in K[x]$ от T. Тогда в алгоритме корреспонденты выбирают случайные относительно равномерного распределения обратимые матрицы $P(A)$ и $P(B)$ из M.

При выборе в качестве K конечного поля $\mathbb{F}_q$ вероятность того, что случайная матрица окажется обратимой, при относительно малом s по отношению к q близка к 1. Объясним это. В [14, Lemma 9 (Invertibility Lemma)] доказано следующее утверждение: Пусть для произвольного поля $\mathbb{F}$ матрицы $T_0, T_1, \ldots, T_r \in M_k(\mathbb{F})$ обладают тем свойством, что их линейная оболочка содержит матрицу из $\mathrm{GL}_k(\mathbb{F})$; S — конечное подмножество в $\mathbb{F}$. Если $\alpha_1, \ldots, \alpha_r$ выбираются равномерно и независимо из S, то вероятность того, что матрица $\alpha_1 T_1 + \ldots + \alpha_r T_r$ обратима, не меньше чем $1 - k/|S|$.

В нашем случае полагаем $\mathbb{F} = \mathbb{F}_q, S = \mathbb{F}_q$, $T_0 = T^0 = E$, $T_1 = T$, $\ldots$, $T_{s-1} = T^{s-1}$. По теореме Кронекера — Капелли бóльшие, чем $s-1$, степени матрицы T линейно выражаются через выписанные степени, поэтому M является линейной оболочкой данного множества матриц. По лемме вероятность случайного выбора из M обратимой матрицы не меньше чем $1 - s/q$.

Следующий протокол представляет схему передачи зашифрованного сообщения от Алисы к Бобу:

— Алиса выбирает параметр k и многочлен $f_\alpha(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k \in K[x]$, $\alpha_0, \alpha_k \in K^*$, определяющий операции дифференцирования и интегрирования. Эти данные секретны.

— Подобным образом поступает и Боб, выбирая параметр m и определяя свои операции многочленом $g_\beta(x) = \beta_0 + \beta_1 x + \ldots + \beta_m x^m \in K[x]$, $\beta_0, \beta_m \in K^*$. Эти данные также секретны. Ключом в данном протоколе служит пара $Key = (f_\alpha(x), g_\beta(x))$.

— Алиса выбирает набор нитей C, состоящий из s наборов констант $\bar{c}_j = (c_{j,0}, \ldots, c_{j,l})$, $j = 1, \ldots, s$, интегрирует вправо в соответствии с этим набором покомпонентно $\bar{A}$, получая $\iota_{\alpha,\bar{C}}(\bar{A})$. Затем она выбирает параметр r и случайную последовательность A' наборов $\bar{a}'_j = (a_{j,-r}, \ldots, a_{j,-1})$, $j = 1, \ldots, s$, и дописывает эти наборы перед соответствующими наборами из $\iota_{\alpha,\bar{C}}(A)$, получая последовательность нитей $(A'||\iota_{\alpha,\bar{C}}(A))$. Далее она выбирает случайную матрицу $P_A \in M$, применяет линейное преобразование с этой матрицей к полученным нитям и пересылает Бобу результат

$$\tilde{A} = (\bar{b}_1, \ldots, \bar{b}_s)$$

— последовательность из s наборов длины $l + 1 + r + k$.

— Боб выбирает набор нитей D, состоящий из s наборов констант $\bar{d}_j = (d_{j,0}, \ldots, d_{j,l})$, $j = 1, \ldots, s$, интегрирует вправо в соответствии с этим набором покомпонентно $\tilde{A}$, получая $\iota_{\beta,\bar{D}}(\tilde{A})$. Далее Боб выбирает параметр t и случайную последовательность $\bar{A}''$ наборов $\bar{a}''_j = (a_{j,-r-t}, \ldots, a_{j,-r-1})$, $j = 1, \ldots, s$, дописывает эти наборы в начало последовательности, получая

$$(A''||\iota_{\beta,\bar{D}}(\tilde{A}).$$

Далее он выбирает случайную матрицу $P_B \in M$, применяет линейное преобразование с этой матрицей к полученным нитям и пересылает Алисе результат

$$\tilde{B} = (f_1, \ldots, f_s)$$

— последовательность наборов длины $l + 1 + r + t + k + m$.

— Алиса удаляет из каждой нити начальный набор из r компонент, дифференцирует покомпонентно полученную последовательность, применяет к нитям линейное преобразование с матрицей P_A^{-1} и передаёт Бобу результат

$$\tilde{A}' = (\bar{g}_0, \ldots, \bar{g}_s)$$

— последовательность наборов длины $l + 1 + t + m$.

— Боб удаляет из каждой нити начальный набор из t компонент, дифференцирует покомпонентно полученную последовательность, применяет к нитям линейное преобразование с матрицей P_B^{-1} и получает сообщение Алисы $\bar{A}$.

Корректность вычислений обусловлена тем, что линейные преобразования перестановочны с дифференцированиями и интегрированиями, дифференцирования перестановочны, а используемые линейные преобразования также перестановочны между собой. Дописывание в начало случайных интервалов с последующим удалением интервалов той же длины не изменяет полученного результата, так как начальные значения при дифференцировании и правом интегрировании не влияют на вычисление последующих компонент. В то же время такая операция затрудняет определение в продифференцированном или проинтегрированном наборе нитей позиции, с которой произведено данное действие. Это также затрудняет применение метода Гаусса.

Основания стойкости зашифрования. В предлагаемом протоколе не содержится механизма аутентификации, поэтому он не защищён от атаки «противник посередине». Для противодействия данной атаке требуются дополнительные средства.

Передаваемое сообщение может быть прочитано взломщиком, если ему удастся найти хотя бы один из многочленов $f_\alpha(x)$ или $g_\beta(x)$. Прежде всего рассмотрим ситуацию, когда известен конечный набор $\bar{a} = (a_0, a_1, \ldots, a_{l+n}$ и результат дифференцирования $i_\alpha(\bar{a}) = (b_0, b_1, \ldots, b_l)$. Эти данные позволяют определить степень k определяющего многочлена $f_\alpha(x)$. Далее можно вычислить коэффициенты этого многочлена, решая систему линейных уравнений

$$\begin{cases} \alpha_0 a_0 + \alpha_1 a_1 + \ldots + \alpha_k a_k = b_0, \\ \alpha_0 a_1 + \alpha_1 a_2 + \ldots + \alpha_k a_{k+1} = b_1, \\ \ldots \\ +\alpha_0 a_{l-k} + \alpha_1 a_{l-k+1} \ldots + \alpha_k a_l = b_l. \end{cases}$$

Вычислительная сложность алгоритма Гаусса, основного метода решения системы из l линейных уравнений, составляет $O(l^3)$. Известные усовершенствования метода Гаусса не дают существенного уменьшения сложности вычислений. В то же время для вычисления компонент интервала длины l при известном определяющем многочлене требуется произвести $O(l)$ операций.

Рекомендуется использовать определяющие многочлены $f_\alpha(x)$ и $g_\beta(x)$ с разреженными множествами ненулевых коэффициентов. При этом сокращается время выполнения необходимых дифференцирований и интегрирований. Аналогичные рассуждения проходят для интегрирований.

В предложенном протоколе описанная ситуация не возникает из-за использования линейных преобразований и дописывания случайных наборов в начало передаваемых последовательностей с последующим удалением начальных наборов той же длины.

3.2. Аутентификация

Приведём описание протокола для схемы, основанной на дискретных дифференцировании и интегрировании. Аутентифицируется Алиса, проверяет Боб.

— Открытые данные Алисы состоят из коммутативного кольца с единицей K, последовательности из s нитей $\bar{A} = (\bar{a}_1, \ldots, \bar{a}_s)$, где $\bar{a}_j = (a_{j,0}, \ldots, a_{j,l}) \in K^{l+1}$, и её значений $\bar{B} = (\delta_{\alpha,\varphi}(A)$ при скрученном дифференцировании с секретными данными — определяющим многочленом $f_\alpha(x) \in K[x]$ и линейным преобразованием нитей φ, заданным матрицей $P_\varphi \in \mathrm{GL}_s(K)$. Эти данные должны либо быть подтверждены

сертификатом удостоверяющего центра, либо переданы Бобу в процессе предварительной начальной регистрации.

— При запросе Боба об аутентификации Алиса выбирает определяющий многочлен $g_\beta(x) \in K[x]$, линейное преобразование ψ, заданное матрицей $P_\psi \in \mathrm{GL}_s(K)$, вычисляет и предъявляет Бобу набор нитей $\bar{C} = \delta_{\beta,\psi}(\bar{B})$.

— Боб посылает Алисе метку c, равную 0 или 1.

— Если $c = 0$, Алиса посылает в ответ параметры скрученного дифференцирования $\delta_{\beta,\psi}$, Боб вычисляет $\bar{C}' = \delta_{\beta,\psi}(B)$ и проверяет справедливость равенства $\bar{C}' = \bar{C}$. Этот раунд аутентификации Алиса проходит, если равенство справедливо.

— Если $c = 1$, Алиса посылает в ответ параметры скрученного дифференцирования $\delta_{\gamma,\phi}$ — суперпозиции скрученных дифференцирований $\delta_{\alpha,\varphi}$ и $\delta_{\beta,\psi}$, Боб вычисляет $\bar{A}' = \delta_{\gamma,\phi}(A)$ и проверяет справедливость равенства $\bar{A}' = \bar{C}$. Этот раунд аутентификации Алиса проходит, если равенство справедливо.

— Подобно алгоритму аутентификации Фиата — Шамира (см., например, [12, с. 408] или [4, с. 143]) противник, не зная параметров скрученного дифференцирования $\delta_{\alpha,\varphi}$, может пройти раунд с $c = 1$, если специальным образом подготовится, а именно: вместо $\bar{C}$ он пошлёт значение $\delta_{\lambda,\xi}(\bar{A})$ для случайных параметров λ и ξ, которые он сможет предъявить при метке $c = 1$. Но тогда он не сможет аутентифицироваться при метке $c = 0$. Если он ожидает метку $c = 0$, то он просто выбирает свои параметры в качестве β и ψ, которые предъявляет при метке $c = 0$. Но тогда он не сможет пройти аутентификацию при метке $c = 0$. Таким образом, противник аутентифицируется с вероятностью $1/2$. Вероятность прохождения q раундов аутентификации равна $(1/2)^q$ и её можно сделать сколь угодно малой за счёт увеличения q.

Приведённая схема аутентификации является схемой с нулевым разглашением: в процессе не раскрывается главный секрет — параметры α и φ. Стойкость схемы основывается на трудноразрешимости задачи вычисления параметров скрученного дифференцирования.

3.3. Распределение ключа

Опишем протокол для схемы распределения ключа типа Диффи — Хеллмана с использованием скрученных дифференцирований. Сначала корреспонденты Алиса и Боб договариваются о выборе коммутативного кольца с единицей K и параметра s. Эти данные открыты. Корреспонденты договариваются также о выборе параметра l и конкретной последовательности из s нитей $\bar{A} = (\bar{a}_1, \ldots, \bar{a}_s)$, где $\bar{a}_j = (a_{j,0}, \ldots, a_{j,l}) \in K^{l+1}$. Эти данные также открыты.

— Алиса выбирает параметр k и многочлен $f_\alpha(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k \in K[x]$, определяющий операцию дифференцирования. Также она выбирает линейное преобразование нитей φ, заданное матрицей $P_A \in \mathrm{GL}_s(K)$. Эти данные секретны. Затем Алиса вычисляет и передаёт Бобу значение

$$K_A = \delta_{\alpha,\varphi}(\bar{A}).$$

— Боб выбирает параметр s и многочлен $g_\beta(x) = \beta_0 + \beta_1 x + \ldots + \alpha_m x^m \in K[x]$, определяющий операцию дифференцирования. Также она выбирает линейное преобразование нитей ψ, заданное матрицей $P_B \in \mathrm{GL}_s(K)$. Эти данные секретны. Затем Боб вычисляет и передаёт Алисе значение

$$K_B = \delta_{\beta,\psi}(\bar{A}).$$

— Алиса вычисляет распределенный ключ

$$K = \delta_{\alpha,\varphi}(K_B).$$

— Боб вычисляет распределенный ключ

$$K = \delta_{\beta,\psi}(K_A).$$

Корректность схемы (равенство значений, полученных на двух последних шагах) определяется перестановочностью операций дифференцирования. Стойкость схемы основывается на трудноразрешимости задачи вычисления параметров скрученного дифференцирования.

Заключение

В работе представлены определения дискретных операций дифференцирования и интегрирования последовательностей элементов произвольного коммутативного кольца с единицей, а также их скрученные версии на наборах таких последовательностей (нитях), использующие линейные преобразования нитей. Определены основные свойства этих операций. Дан краткий обзор их применений. В частности, предложены схемы передачи сообщения, распределения ключа и аутентификации с использованием этих операций.

ЛИТЕРАТУРА

1. *Волошин С. К., Романьков В. А.* Обобщенные дискретные операции дифференцирования и интегрирования // Вестник Омского университета. 2021. Т. 26. № 4. С. 4–8.
2. *Романьков В. А.* Обобщённая схема скрытого компактного хранения данных различных пользователей в общей открытой базе // Известия Иркутского государственного университета. Сер. Математика. 2022. Т. 20. С. 1–14.
3. *Романьков В. А.* О скрытом компактном способе хранения данных // Прикладная дискретная математика. Приложение. 2020. № 13. С. 56–59.
4. *Roman'kov V.* Embedding theorems for solvable groups // Proc. AMS. 2021. V. 149. P. 4133–4143.
5. *Neumann P. M.* On the structure of standard wreath products of groups // Math. Z. 1964. V. 84. P. 343–373.
6. *Романьков В. А.* Криптографический анализ некоторых схем шифрования, использующих автоморфизмы // Прикладная дискретная математика. 2013. № 3(21). С. 35–51.
7. *Myasnikov A. and Roman'kov V.* A linear decomposition attack // Groups Complexity Cryptology. 2015. V. 7. No. 1. P. 81–94.
8. *Roman'kov V. A.* A nonlinear decomposition attack // Groups Complexity Cryptologogy. 2017. V. 8. No. 2. P. 197–207.
9. *Roman'kov V.* Essays in algebra and cryptology: Algebraic cryptanalysis. Omsk: Omsk State University, 2018. 208 p.
10. *Романьков В. А.* Алгебраическая криптология. Омск: ОмГУ, 2020. 261 с.
11. *Ben-Zvi A., Kalka A., and Tsaban B.* Cryptanalysis via algebraic spans // Proc. 38th Ann. Intern. Cryptology Conf. Santa Barbara, CA, USA, 2018. Part 1. P. 255–274.
12. *Menezes A. J., Oorschot P. C., and Vanstone S.* Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996. 816 p.
13. *Романьков В. А.* Введение в криптографию. Курс лекций. М.: Форум, 2012. 239 с.
14. *Tsaban B.* Polynomial time solutions of computational problems in noncommutative algebraic cryptography // J. Cryptology. 2015. V. 28. No. 3. P. 601–622.

REFERENCES

1. *Voloshin S. K. and Roman'kov V. A.* Obobshchennye diskretnye operatsii differentsirovaniya i integrirovaniya [Generalized discrete operations of differentiation and integration.] Vestnik OmSU, 2021, vol. 26, no. 4, pp. 4–8. (in Russian)
2. *Roman'kov V. A.* Obobshchennaya skhema skrytogo kompaktnogo khraneniya dannykh razlichnykh pol'zovateley v obshchey otkrytoy baze [Generalized scheme of hidden compact storage of data of various users in a common open database]. Izvestiya ISU. Matematika, 2022, vol. 20, pp. 1–14. (in Russian)
3. *Roman'kov V. A.* O skrytom kompaktnom sposobe khraneniya dannykh [About the hidden compact way to store data]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2020, no. 13, pp. 56–59. (in Russian)
4. *Roman'kov V.* Embedding theorems for solvable groups. Proc. AMS, 2021, vol. 149, pp. 4133–4143.
5. *Neumann P. M.* On the structure of standard wreath products of groups. Math. Z., 1964, vol. 84, pp. 343–373.
6. *Roman'kov V. A.* Kriptograficheskiy analiz nekotorykh skhem shifrovaniya, ispol'zuyushchikh avtomorfizmy [Cryptanalysis of some schemes applying automorphisms]. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 35–51. (in Russian)
7. *Myasnikov A. and Roman'kov V.* A linear decomposition attack. Groups Complexity Cryptology, 2015, vol. 7, no. 1, pp. 81–94.
8. *Roman'kov V. A.* A nonlinear decomposition attack. Groups Complexity Cryptology, 2017, vol. 8, no. 2, pp. 197–207.
9. *Roman'kov V.* Essays in Algebra and Cryptology: Algebraic Cryptanalysis. Omsk, OmskSU Publ., 2018. 208 p.
10. *Roman'kov V. A.* Algebraicheskaya Kriptologiya [Algebraic Cryptology]. Omsk, OmSU Publ., 2020. 261 p. (in Russian)
11. *Ben-Zvi A., Kalka A., and Tsaban B.* Cryptanalysis via algebraic spans. Proc. 38th Ann. Intern. Cryptology Conf., Santa Barbara, CA, USA, 2018, part 1, pp. 255–274.
12. *Menezes A. J., Oorschot P. C., and Vanstone S.* Handbook of Applied Cryptography. Boca Raton, CRC Press, 1996. 816 p.
13. *Roman'kov V. A.* Vvedenie v kriptografiyu. Kurs lektsiy [Introduction to Cryptography. Lecture Course]. Moscow, Forum, 2012. 239 p. (in Russian)
14. *Tsaban B.* Polynomial time solutions of computational problems in noncommutative algebraic cryptography. J. Cryptology, 2015, vol. 28, no. 3, pp. 601–622.