ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ МОЛДОВЫ

ДОКТОРСКАЯ ШКОЛА ФИЗИКО-МАТЕМАТИЧЕСКИХ, ИНФОРМАЦИОННЫХ И ТЕХНИЧЕСКИХ НАУК

На правах рукописи
УДК: 519.21:004.421(043.2)

МАЛЮТИНА НАДЕЖДА

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАЗРАБОТКЕ КРИПТОГРАФИЧЕСКИХ И АЛГЕБРАИЧЕСКИХ АЛГОРИТМОВ

Автореферат докторской диссертации по информатике

122.03 – Моделирование, Математические Методы, Программное Обеспечение

Автор: Малютина Надежда

Научные руководители: Корлат Андрей, доктор физико-математических наук, профессор университар

Щербаков Виктор, доктор хабилитат физико-математических наук, профессор университар

Научные консультанты: Кожокару Светлана, доктор хабилитат информатики, член-корреспондент

Арнаутов Владимир, доктор хабилитат физико-математических наук, академик

Цицкиев Инга, доктор информатики, конференциар университар

КИШИНЕВ, 2023

Диссертация разработана в Докторской школе физико-математических, информационных и технических наук Государственного Университета Молдовы.

Докторская комиссия:

Председатель комиссии:	**ГАЙНДРИК Константин,** доктор хабилитат информатики, член-корреспондент, Институт Математики и Информатики им. Владимира Андрунакиевича, Государственный Университет Молдовы;
Научные руководители:	**КОРЛАТ Андрей**, доктор физико-математических наук, профессор университар, Технический университет Молдовы;
	ЩЕРБАКОВ Виктор, доктор хабилитат физико-математических наук, профессор университар, Институт Математики и Информатики им. Владимира Андрунакиевича, Государственный Университет Молдовы;
Официальные оппоненты:	**КИРИЯК Любомир,** доктор хабилитат физико-математических наук, профессор университар, Государственный педагогический университет им. Иона Крянгэ;
	ЦИЦКИЕВ Инга, доктор информатики, конференциар университар, Институт математики и информатики им. Владимира Андрунакиевича, Государственный Университет Молдовы;
	ОХРИМЕНКО Сергей, доктор хабилитат экономических наук, профессор университар, Академия Экономических наук Молдовы;
	ПЕТИК Мирча, доктор информатики, конференциар университар, Государственный университет им. Алеку Руссо, г. Бельцы;
Ученый секретарь:	**НОВАК Людмила,** доктор физико-математических наук, конференциар университар, Государственный университет Молдовы.

Защита диссертации состоится 21.04.2023 в 14-00 на заседании докторской комиссии в Институте Математики и Информатики им. Владимира Андрунакиевича, ул. Академическая 5, ауд. 340.

С диссертацией и авторефератом можно ознакомиться в библиотеке Государственного Университета Молдовы и на веб-сайте Национального Агентства по обеспечению качества в области образования и исследований (www.cnaa.md).

Автореферат разослан 13 марта 2023

Ученый секретарь: _____ Новак Людмила

Автор: _____ Малютина Надежда

© Малютина Надежда, 2023

СОДЕРЖАНИЕ

1. КОНЦЕПТУАЛЬНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЯ 4
2. СОДЕРЖАНИЕ РАБОТЫ 8
3. ОБЩИЕ ВЫВОДЫ И РЕКОМЕНДАЦИИ 22
ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА 27
АННОТАЦИЯ 31
ADNOTARE 32
ANNOTATION 33

1. КОНЦЕПТУАЛЬНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЯ

Актуальность и важность исследования. Большинство известных конструкций кодов обнаружения и исправления ошибок, криптографических алгоритмов и систем шифрования используют ассоциативные алгебраические структуры, такие как группы и поля [1, 2]. Анализ исследований показал, что можно использовать такие неассоциативные структуры, как квазигруппы, во многих отраслях теории кодирования, и особенно в криптологии. Коды и шифры на основе неассоциативных систем демонстрируют лучшие возможности, чем известные коды и шифры на основе ассоциативных систем [3, 4].

Первыми профессиональными криптографами, которые занимались развитием теории квазигрупп, были: А.А. Альберт, А. Дриско, М. М. Глухов, Дж.Б. Россер, Э. Шёнхардт, Х. Дж. Мендельсон и Р. Шауфлер. Некоторые результаты, полученные в области применения квазигрупп в криптологии и теории кодирования, описаны в работах Дж. Денеса и А.Д. Кидвелла [3, 5-7]. Многие результаты неассоциативной криптографии с открытым ключом можно найти у А. Калки [8].

Важные результаты в применении теории квазигрупп в криптографии были получены М.Э. Тужилиным [9]; Ю.М. Мовсисяном [10]; А.В. Грибовым, П.А. Золотых и А.В. Михалевым [11]; Дж. Мейз, К. Моника и И. Розенталем [12]; В.Шпильрайном и А. Ушаковым [13]; Р.Э. Атани, Ш.Э. Атани и С. Мирзакучаки [14]; А. Крапежем [15, 16]; К.А. Мейером [17]; В.А. Артамоновым, С. Чакрабарти, В.Т. Марковым и С.К. Полом [18, 19].

Ч. Кошельны и Г.Л. Маллен представили криптосистему с открытым ключом, использующую обобщенные поточные шифры, основанные на квазигруппах [20]. Квазигруппы для безопасного кодирования предложили использовать Э. Оходкова и В. Снасель [21]; С. Марковски, Д. Глигороски, Б. Стойцевска и В. Бакева [22, 23]; С. Марковски, В. Димитрова, З. Трайческа, М. Петковска, М. Костадиноски и Д. Бухов [24].

С. Марковски и его соавторы представили поточный шифр с почти открытым ключом, основанный на квазигруппах [22]. Алгоритм Марковского и его обобщения в настоящее время широко известны и часто используются для построения поточных шифров на основе квазигрупп. Усовершенствования и исследования алгоритма Марковского интенсивно проводились В.А. Щербаковым [25].

Важные результаты были получены А. Крапежем, В. Бакевой, В. Димитровой и А. Поповской-Митровики [26-28]. А. Крапеж и Д. Живкович предлагают использовать парастрофические преобразования квазигрупп и их модификации, которые весьма

перспективны для применения и исследования [29]. Криптоанализ этих шифров изучался в диссертационной работе М. Войводы [30].

Некоторые обобщения и модификации алгоритма Марковского можно найти в работах В.А. Щербакова и А. Петреску [31-35]. Дальнейшее развитие алгоритма Марковского представляется в работах С. Марковского, Д. Глигороски, Л. Коцарева, С. Й. Кнапскога, М. Хассинена [36-38], С. Чакрабарти, Сейбал К. Пал и С. Гангопадхья [39].

Важные сведения о криптоанализе некоторых поточных шифров можно найти в статье В.А. Щербакова и П. Ксорго [40].

Алгоритм Марковского имеет множество различных обобщений и может быть использован для построения аналогов схемы Эль-Гамаля. Аналог системы шифрования Эль-Гамаля на основе алгоритма Марковского приведен в работах В.А. Щербакова и Н.А. Молдовяна [41]; А.В. Грибова [42].

Криптографические методы стали широко использоваться в электронной коммерции, телекоммуникациях и многих других средах. Эти методы используются не только для шифрования транзакций и контроля над производством криптовалют, но и обеспечивают безопасную работу банковских систем, пластиковых карт, банкоматов, беспроводных устройств и т.д.

Современная криптография занимается такими проблемами защиты информации, как конфиденциальность, целостность, аутентификация, невозможность отказа сторон от авторства и управление ключами. Создание надежных алгоритмов шифрования является ключевой задачей защиты информации. Поэтому любой построенный алгоритм необходимо подвергать тщательному анализу с целью выявления его слабых мест и возможности взлома.

В диссертации поднимаются следующие вопросы:

Задача 1. Исследовать и построить алгоритмы на основе алгоритма Марковского с использованием квазигрупп и группоидов.

Задача 2. Провести криптоанализ шифров, построенных с использованием обобщенных алгоритмов.

Задача 1 обсуждается в Главе 2, а задача 2 — в Главах 3 и 4.

Цель и задачи диссертации. Целью научного исследования является построение новых и усовершенствование уже разработанных криптографических алгоритмов на основе алгоритма Марковского, проведение их криптоанализа и написание программ, реализующих работу этих алгоритмов.

Для достижения этой цели были определены следующие задачи:

- Разработка эффективного криптографического алгоритма на основе алгоритма Марковского с использованием левой и правой бинарных квазигрупп и n-арных группоидов;
- Разработка программ, реализующих работу построенных алгоритмов;
- Проведение атак на все изученные и построенные шифры;
- Осуществление сравнительного анализа всех проведенных атак;
- Нахождение текстов минимальной длины для всех изученных типов атак.

Гипотеза исследования. Классический алгоритм Марковского может служить базой для построения новых обобщений на основе бинарных квазигрупп и обратимых на одном фиксированном месте группоидов. Построенные обобщенные алгоритмы будут иметь более высокую степень стойкости к известным видам атак. Криптоанализ шифров, построенных с использованием обобщенных алгоритмов, представляет собой интересную область исследований для криптоаналитиков.

Прикладные методы исследования. В данной работе применяется анализ научной литературы и практического опыта, проводится систематизация ранее полученных результатов по проблеме исследования. Сравниваются существующие подходы к решению поставленных задач и современные методы построения криптографических алгоритмов на основе неассоциативных структур и их свойств, и, в частности, методы неассоциативной алгебры, включая методы построения n-арных группоидов, а также классические методы криптоанализа. Исследование основано на использовании классического алгоритма Марковского и его обобщений.

Объектом исследования являются обобщенные алгоритмы Марковского, основанные на бинарных квазигруппах и n-арных группоидах.

Научная новизна и оригинальность. Все результаты работы новые и оригинальные. Они представляют собой продолжение предыдущих исследований в этой области. Были разработаны и обобщены алгоритмы, позволившие улучшить работу классического алгоритма Марковского, построены атаки на шифры с использованием обобщенных алгоритмов, а также показана степень стойкости этих шифров. Результаты, представленные в диссертации, представляют интерес для изучения криптологами.

Важная научная решаемая в исследовании задача состоит в разработке новых модификаций классического алгоритма, способствующих повышению стойкости построенного шифра к известным видам атак.

Теоретическая значимость состоит в получении новых улучшенных алгоритмов и шифров, с помощью применения неассоциативных структур, таких как n -арные группоиды, в информатике. Разработанные алгоритмы позволили с новой точки зрения подойти к проблемам, связанным с кодированием и криптоанализом.

Прикладное значение диссертации. Предложены новые модификации алгоритмов кодирования с использованием левых квазигрупп, правых квазигрупп и обратимых на одном месте n-арных группоидов. Разработанные методы позволили решить поставленные задачи и обозначили круг дальнейших вопросов, на которые еще предстоит ответить. Прикладное значение работы заключается в использовании полученных результатов в научных исследованиях, связанных с кодированием данных, изучением эффективности представления информации, криптоанализом данных. Они также могут быть использованы при разработке специализированных курсов для студентов, магистров и докторантов, связанных с изучением криптологии на абстрактных алгебраических структурах.

Результаты представленной диссертации внедрены в работу научно-исследовательской лаборатории «Алгебра и ее приложения» Приднестровского государственного университета им. Т.Г. Шевченко (Тирасполь).

Публикации по теме диссертации и личный вклад. Результаты исследования опубликованы в 21 научной работе, в том числе 7 статей в рецензируемых журналах (2 статьи без соавторов), 8 статей в материалах научных конференций (6 статей без соавторов) и 6 тезисов на научных конференциях (2 тезиса без соавторов).

Непосредственно автором разработано математическое и алгоритмическое обеспечение шифрования и дешифрования текстов, построенных на основе обобщенных алгоритмов Марковского, а также проведен криптоанализ всех построенных шифров.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, общих выводов и рекомендаций, библиографии из 201 источника, 3 приложений, 217 страниц (в том числе 145 страниц основного текста), 1 рисунка и 71 таблицы.

Ключевые слова: алгоритм Марковского, квазигруппа, левая и правая квазигруппа, трансляция, открытый текст, зашифрованный текст, атака, ключ, шифрование, дешифрование.

2. СОДЕРЖАНИЕ РАБОТЫ

Структура диссертации представлена четырьмя главами, которые содержат теоретические и практические результаты, полученные при изучении и построении обобщений алгоритма Марковского, а также при их криптоанализе.

Во введении формулируются актуальность и значимость темы исследования, определяется объект исследования, формулируются цель и задачи исследования, определяются методы исследования, раскрывается научная новизна, теоретическая и практическая значимость диссертации. Изучаемая научная проблема представлена с акцентом на важность прикладной ценности работы. Сформулированы основные положения к защите, приведены сведения об апробации и внедрении результатов. Представлен краткий анализ выступлений и публикаций по теме диссертации. В конце этого раздела приводится краткое изложение содержания работы.

Первая глава «Текущая ситуация в области использования информационных технологий при разработке криптографических и алгебраических алгоритмов», состоящая из семи параграфов, носит вводный характер. В ней представлен обзор текущего состояния наиболее важных областей современной криптографии для нашей работы. Описаны основные понятия криптологии, необходимые для изложения работы. Проведен анализ одной из наиболее часто используемых классификаций криптографических алгоритмов и отмечено, каким условиям должны удовлетворять современные алгоритмы шифрования. Анализируются основные особенности и проблемы симметричного и асимметричного шифрования. Выявлены преимущества и недостатки, характерные для современных симметричных и асимметричных систем. Описаны наиболее популярные функции хэширования и цифровые подписи. Особое внимание уделено существующим на сегодняшний день криптоаналитическим методам. Сделан обзор применения неассоциативных алгебраических структур в криптологии, в котором основное внимание уделено алгоритму Марковского и его построенным на сегодняшний день обобщениям.

Во второй главе «Алгоритм Марковского и его новые обобщения» изучается работа алгоритма Марковского для бинарных квазигрупп и особенности работы алгоритма для левой и правой квазигрупп. Построены обобщения алгоритма Марковского для обратимых группоидов на любом фиксированном месте. Эти алгоритмы были построены

совместно с В.А. Щербаковым. Глава состоит из восьми параграфов, в которых достигается цель 1.

Первые три параграфа посвящены результатам, полученным при изучении алгоритма Марковского в случае использования бинарных квазигрупп. Показано, что алгоритм для левой квазигруппы ничем не отличается от традиционного алгоритма Марковского. Указана особенность алгоритма Марковского для правой квазигруппы. Разработаны программы, реализующие работу этих алгоритмов. Полученные программы работают для шифрования и расшифровки текстов заданной длины (длина текста может быть легко изменена). Программы работают при любых значениях лидеров (лидеров выбирает пользователь). С помощью этих программ можно построить реализацию алгоритма Марковского для любой бинарной квазигруппы.

Помимо бинарных квазигрупп в этой конструкции могут использоваться также n-арные квазигруппы и их парастрофы [43, 25].

Параграф 2.4. диссертации посвящен построению Обобщенного Алгоритма 1.

Мы определим n -арную операцию f на множестве Q как $(n+1)$ -кортежи следующего вида $\big(x_1, x_2, \dots, x_n, f(x_1, x_2, \dots, x_n)\big)$, где $x_1, x_2, \dots, x_n, f(x_1, x_2, \dots, x_n) \in Q$.

Определение 2.4.1. *n-арным группоидом* (Q, f) называется непустое множество Q вместе с определенной на нем n-арной операцией f.

Определение 2.4.2. n-арный группоид (Q, f) называется обратимым на *i-м месте*, $i = \overline{1,n}$, если уравнение: $f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n) = a_{n+1}$ однозначно разрешимо для любых элементов: $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n, a_{n+1} \in Q$ [43].

В этом случае обратная операция ${}^{(i,n+1)}f(a_1, \dots, a_{i-1}, a_{n+1}, a_{i+1}, \dots, a_n) = x_i$ определяется единственным образом и мы имеем:

$$\left.\begin{matrix} f\big(a_1, \dots, a_{i-1}, {}^{(i,n+1)}f(a_1, \dots, a_{i-1}, a_{n+1}, a_{i+1}, \dots, a_n), a_{i+1}, \dots, a_n\big) = a_{n+1} \\ {}^{(i,n+1)}f(a_1, \dots, a_{i-1}, f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n), a_{i+1}, \dots, a_n) = x_i \end{matrix}\right\}. \qquad (\mathbf{2.1})$$

Определение 2.4.3. *n-арной квазигруппой* называется n-арный группоид (Q, f) с n-арной операцией f такой что в равенстве $f(x_1, x_2, \dots, x_n) = x_{n+1}$ факт знания любых n элементов $\{x_1, x_2, \dots, x_n, x_{n+1}\}$ однозначно определяет оставшийся один элемент [43, 25].

Определение 2.4.4. n-арный группоид (Q, f) называется *n -арной квазигруппой* , если на множестве Q существуют операции ${}^{(1,n+1)}f, {}^{(2,n+1)}f, \dots, {}^{(n,n+1)}f$ такие, что в алгебре $(Q, f, {}^{(1,n+1)}f, {}^{(2,n+1)}f, \dots, {}^{(n,n+1)}f)$ следующие тождества выполняются для всех $i = \overline{1,n}$:

$$\left.\begin{matrix} f\left(x_1,\dots,x_{i-1},{}^{(i,n+1)}f(x_1,\dots,x_n),x_{i+1},\dots,x_n\right)=x_i \\ {}^{(i,n+1)}f(x_1,\dots,x_{i-1},f(x_1,\dots,x_n),x_{i+1},\dots,x_n)=x_i \end{matrix}\right\} \quad (\mathbf{2.2})$$

Ясно, что число i-обратимых n-арных группоидов (число n фиксировано) больше, чем число n-арных квазигрупп (число n фиксировано). Этот факт послужил толчком к построению новых обобщений алгоритма Марковского.

Алгоритм 2.4.5. (Обобщенный алгоритм 1). Пусть Q непустой конечный алфавит и $k-$ натуральное число, $u_j, v_j \in Q, j \in \{1,\dots k\}$.

Определим n-арный группоид (Q,f), который обратим на i-м месте, $i=\overline{1,n}$. Тогда группоид $(Q,{}^{(i,n+1)}f)$ будет определен однозначно. В этом случае имеет место равенство:

$${}^{(i,n+1)}f(v_1,\dots,v_{i-1},v_n,v_i,\dots,v_{n-1}) =$$

$$= {}^{(i,n+1)}f(v_1,\dots,v_{i-1},f(v_1,\dots,v_{i-1},u_n,v_i,\dots,v_{n-1}),v_i,\dots,v_{n-1}) = u_n.$$

Возьмем фиксированные элементы $l_1^{(n-1)^2}\left(l_1,l_2,\dots l_{(n-1)^2}\in Q\right)$, которые назовем лидерами.

Пусть $u_1,u_2,\dots u_k-$ кортеж из k букв алфавита Q.

Предлагается следующая *процедура шифрования*:

$v_1=f(l_1,l_2,\dots,l_{i-1},u_1,l_i,\dots,l_{n-1})$,

$v_2=f(l_n,l_{n+1},\dots,l_{n+i-2},\ u_2,l_{n+i-1},\dots,l_{2n-2})$,…,

$v_{n-1}=f\left(l_{n^2-3n+3},\dots,\ l_{n^2-3n+1+i},u_{n-1},l_{n^2-3n+2+i},\dots,l_{(n-1)^2}\right)$,

$v_n=f(v_1,\dots,v_{i-1},u_n,v_i,\dots,v_{n-1})$,

$v_{n+1}=f(v_2,\dots,v_i,u_{n+1},v_{i+1},\dots,v_n)$,

$v_{n+2}=f(v_3,\dots,v_{i+1},u_{n+2},v_{i+2},\dots,v_{n+1})$,… .

Алгоритм расшифровки строится аналогично бинарному случаю и имеет вид:

$u_1={}^{(i,n+1)}f(l_1,l_2,\dots,l_{i-1},v_1,l_i,\dots,l_{n-1})$,

$u_2={}^{(i,n+1)}f(l_n,l_{n+1},\dots,l_{n+i-2},\ v_2,l_{n+i-1},\dots,l_{2n-2})$,…,

$u_{n-1}={}^{(i,n+1)}f(\ l_{n^2-3n+3},\dots,\ l_{n^2-3n+1+i},v_{n-1},l_{n^2-3n+2+i},\dots,l_{(n-1)^2})$,

$u_n={}^{(i,n+1)}f(v_1,\dots,v_{i-1},v_n,v_i,\dots,v_{n-1})$,

$u_{n+1}={}^{(i,n+1)}f(\ v_2,\dots,v_i,v_{n+1},v_{i+1},\dots,v_n)$,

$u_{n+2}={}^{(i,n+1)}f(v_3,\dots,v_{i+1},v_{n+2},v_{i+2},\dots,v_{n+1})$,…

Для обратимого на последнем месте группоида (частный случай, когда $i=n$) алгоритм шифрования принимает вид:

$v_1=f(l_1,l_2,\dots,l_{n-1},u_1)$,

$v_2 = f(l_n, l_{n+1}, \dots, l_{2n-2}, u_2)$, …,

$v_{n-1} = f\left(l_{n^2-3n+3}, \dots, l_{(n-1)^2}, u_{n-1}\right)$,

$v_n = f(v_1, \dots, v_{n-1}, u_n)$,

$v_{n+1} = f(v_2, \dots, v_n, u_{n+1})$,

$v_{n+2} = f(v_3, \dots, v_{n+1}, u_{n+2})$, … .

Алгоритм дешифровки в этом случае будет выглядеть следующим образом:

$u_1 = {}^{(n,n+1)}f(l_1, l_2, \dots, l_{n-1}, v_1)$,

$u_2 = {}^{(n,n+1)}f(l_n, l_{n+1}, \dots, l_{2n-2}, v_2)$,…,

$u_{n-1} = {}^{(n,n+1)}f(l_{n^2-3n+3}, \dots, l_{(n-1)^2}, v_{n-1})$,

$u_n = {}^{(n,n+1)}f(v_1, \dots, v_{n-1}, v_n)$,

$u_{n+1} = {}^{(n,n+1)}f(v_2, \dots, v_n, v_{n+1})$,

$u_{n+2} = {}^{(n,n+1)}f(v_3, \dots, v_{n+1}, v_{n+2})$,… .

В работе приведена программная реализация шифрования и дешифрования с использованием Обобщенного Алгоритма 1. Длина текста задается в начале программы, затем вводятся значения лидеров. Таблица шифрования или дешифрования вводится для каждого случая индивидуально, после чего происходит обработка открытого текста или зашифрованного текста.

Замечание 2.4.9. Важным условием корректной работы алгоритма является однозначное указание значения подстановки на месте обратимости операции.

Сложность алгоритма возрастает с ростом арности используемой операции.

Полученный Обобщенный Алгоритм 1 в свою очередь можно модифицировать. Для этого воспользуемся таким понятием, как трансляция.

Параграф 2.5. диссертации посвящен построению Обобщенного Алгоритма 2 с использованием трансляций различных степеней.

Трансляция i -обратимого n -арного группоида (Q, f) $(n > 2)$ обозначается так: $T(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n)$, где $a_i \in Q$ для всех $i = \overline{1,n}$ и $T(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n)x = f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$ для всех $x \in Q$.

Из определения i -обратимого n -арного группоида (Q, f) следует, что любая трансляция n -арного группоида (Q, f) это некоторая перестановка элементов из Q. Следующая лемма будет выполняться для любого значения индекса i.

Лемма 2.5.1. Если ${}_fT(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n)$ трансляция i -обратимого n -арного группоида (Q, f), то ${}_fT^{-1}(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n) = {}_{(i,n+1)_f}T(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n)$.

Алгоритм 2.5.2. (Обобщенный Алгоритм 2). Пусть Q непустой конечный алфавит и k – натуральное число, $u_j, v_j \in Q, j \in \{1, \dots k\}$. Определим n-арный группоид (Q, f), который обратим на i-м месте. Ясно, что группоид $(Q, {}^{(i,n+1)}f)$ будет определен единственным образом.

Возьмем фиксированные элементы: $l_1^{(n^2-n)/2}\left(l_1, l_2, \dots l_{(n^2-n)/2} \in Q\right)$, в качестве лидеров.

Пусть $u_1, u_2, \dots u_k$ – кортеж k букв из алфавита Q и $a, b, c, d \dots$ натуральные числа (степени трансляций).

Получим алгоритм шифрования вида:

$v_1 = T^a(l_1, l_2, \dots, l_{i-2}, l_{i-1}, u_1^a, l_i, \dots, l_{n-1})$,

$v_2 = T^b(l_n, l_{n+1}, \dots, l_{n+i-3}, v_1, u_2^b, l_{n+i-2}, \dots, l_{2n-3})$,

$v_3 = T^c(l_{2n-2}, l_{2n-1}, \dots, l_{2n-i+4}, v_1, v_2, u_3^c, l_{2n-i+3}, \dots, l_{3n-6})$, …,

$v_{n-1} = T^d(l_{(n^2-n)/2}, v_1, \dots, v_{i-2}, u_{n-1}^d, v_{i-1}, \dots, v_{n-2})$,

$v_n = T^e(v_1, v_2, \dots, v_{i-1}, u_n^e, v_i, \dots, v_{n-1})$,

$v_{n+1} = T^f(v_2, v_3, \dots, v_i, u_{n+1}^f, v_{i+1}, \dots, v_n), \dots$.

В алгоритме использовались следующие обозначения:

$u_1^a = \underbrace{f(f \dots f(l_1, l_2, \dots, l_{i-2}, l_{i-1}, u_1, l_i, \dots, l_{n-1}) \dots)}_{a \text{ раз}}$,

$u_2^b = \underbrace{f(f \dots f(\ l_n, l_{n+1}, \dots, l_{n+i-3}, v_1, u_2, l_{n+i-2}, \dots, l_{2n-3}) \dots)}_{b \text{ раз}}$,

$u_3^c = \underbrace{f(f \dots f(\ l_{2n-2}, l_{2n-1}, \dots, l_{2n-i+4}, v_1, v_2, u_3, l_{2n-i+3}, \dots, l_{3n-6}) \dots)}_{c \text{ раз}}$, …,

$u_n^e = \underbrace{f(f \dots f(\ v_1, v_2, \dots, v_{i-1}, u_n, v_i, \dots, v_{n-1}) \dots)}_{e \text{ раз}}$, … .

Учитывая Лемму 2.5.1 можно сказать, что алгоритм дешифрования для Обобщенного Алгоритма 2 может быть построен аналогично алгоритму дешифрования, данному для Обобщенного Алгоритма 1 [25].

Для n-арного группоида, обратимого на n-м месте, алгоритм дешифрования будет иметь вид:

$u_1 = (T^a)^{-1}(l_1, l_2, \dots, l_{n-1}, v_1)$,

$u_2 = (T^b)^{-1}(l_n, l_{n+1}, \dots, l_{2n-3}, v_1, v_2)$,…,

$u_{n-1} = (T^c)^{-1}(l_{(n^2-n)/2}, v_1, \dots, v_{n-2}, v_{n-1})$,

$u_n = (T^d)^{-1}(v_1, v_2, \dots, v_{n-1}, v_n)$,

$u_{n+1} = (T^e)^{-1}(v_2, v_3, \dots, v_n, v_{n+1})$,

$u_{n+2} = (T^f)^{-1}(v_3, v_4, \dots, v_{n+1}, v_{n+2}), \dots$.

Особенности Обобщенных алгоритмов иллюстрируются примерами, приведенными в диссертации.

Замечание 2.5.6. Важной задачей в Обобщенном Алгоритме 2 является определение обратных трансляций для процедуры дешифрования.

В работе приведена программная реализация шифрования и дешифрования с использованием Обобщенного Алгоритма 2. Сравнение программ для двух обобщенных алгоритмов приводит к выводу, что программы для второго алгоритма намного сложнее и объемнее. Сложность программ в первую очередь зависит от степени используемых трансляций.

Сравнивая построенные два алгоритма, видим, что общее количество необходимых лидеров для первого алгоритма будет: $(n-1)^2$, а для второго алгоритма искомое количество лидеров будет равно: $\frac{(n-1)n}{2}$. Второе число меньше первого на величину: $(n-1)\left(\frac{n}{2}-1\right)$.

Обобщенный Алгоритм 2 будет намного сложнее, если помимо первой и второй степени трансляций использовать другие степени. Особый интерес представляет определение обратных трансляций для всех используемых в Обобщенном Алгоритме 2. Учитывая все эти отличия и особенности, можно сделать вывод, что наибольший интерес для криптоанализа представляет именно второй алгоритм.

В последних двух параграфах этой главы представлены исследования, связанные с обобщением схемы Эль-Гамаля на основе алгоритма Марковского.

Обычно классическая система шифрования Тахера-Эль-Гамаля формулируется на языке теории чисел с использованием умножения по модулю простого числа [44]. Схема Эль-Гамаля представляет собой криптосистему с открытым ключом, основанную на сложности вычисления дискретных логарифмов в конечном поле.

Для удобства дальнейшего изложения напомним определение изотопии, которое использовалось при построении обобщенной схемы Эль-Гамаля.

Определение 2.1.6. *Операция B изотопна операции A*, если $\exists\, \alpha, \beta, \gamma -$ подстановки множества Q, такие, что: $B(x,y) = \gamma^{-1}A(\alpha x, \beta y) \quad \forall x, y \in Q$, $T = (\alpha, \beta, \gamma)$ —это *изотопия*, а $\alpha, \beta, \gamma -$ это *левая, правая и главная компоненты изотопии* соответственно.

В параграфе 2.7. рассмотрен аналог системы шифрования Эль-Гамаля на основе алгоритма Марковского.

Пусть (Q, f) бинарная квазигруппа $T = (\alpha, \beta, \gamma)$ ее изотопия.

Ключи Алисы будут следующие:

Открытый ключ: $(Q, f), T, T^{(m,n,k)} = (\alpha^m, \beta^n, \gamma^k), m, n, k \in \mathbb{N}$ и алгоритм Марковского.

Закрытый ключ: m, n, k.

Ключи Боба будут следующие:

Открытый ключ: $(Q, f), T, T^{(r,s,t)} = (\alpha^r, \beta^s, \gamma^t), r, s, t \in \mathbb{N}$ и алгоритм Марковского.

Закрытый ключ: r, s, t.

Шифрование.

Чтобы отправить сообщение $b \in (Q, f)$ Боб вычисляет $T^{(r,s,t)}$ для тройки случайных чисел $r, s, t \in \mathbb{N}$.

Затем, зная $T^{(m,n,k)}$ он вычисляет $T^{(mr,ns,kt)}$ и $(T^{(mr,ns,kt)}(Q, f))$.

Чтобы зашифровать сообщение b Боб использует известный Алисе алгоритм Марковского.

Получает зашифрованный текст и свою степенную изотопию: $(T^{(r,s,t)}, (T^{(mr,ns,kt)}(Q, f))b)$.

Дешифрование.

Алиса, зная свои числа m, n, k, после получения зашифрованного текста $(T^{(r,s,t)}, (T^{(mr,ns,kt)}(Q, f))b)$ вычисляет $(T^{(mr,ns,kt)}(Q, f))^{-1}$, используя $T^{(r,s,t)}$, и затем уже вычисляет b.

Пример работы этой схемы приведен в диссертации.

В разработанном алгоритме можно использовать изострофию [45] вместо изотопии, алгоритм из [25] вместо алгоритма Марковского и n-арные квазигруппы $(n > 2)$ [35] вместо бинарных.

Следующим шагом после построения алгоритма является его криптоанализ, с помощью которого можно будет сделать выводы о его надежности и качестве.

Третья глава «Криптоанализ некоторых потоковых шифров (бинарный случай)» состоит из пяти параграфов и выполняет задачу, связанную с криптоанализом шифров, построенных во второй главе с использованием бинарных квазигрупп. Это решает задачу 2.

Для бинарных квазигрупп М. Войвода провел свои атаки, и автор диссертации показывает, как можно улучшить эти результаты (провести усеченные атаки), кроме того, автор предлагает свои модифицированные атаки, которые показывают лучшие результаты, чем атаки М. Войводы. Для каждого случая определяется минимальное количество символов, необходимое для успешной атаки. Анализируются предельные соотношения количества символов, используемых в различных видах атак.

М. Войвода провел криптоанализ системы кодирования файлов на основе бинарных квазигрупп [46, 30] и показал, как взломать этот шифр, используя атаку только зашифрованным текстом [46]. В его статье описан исследуемый поточный шифр, а также обобщены результаты, изученные на тот момент по шифрам в области криптоанализа.

В параграфах 3.1. и 3.2. показано, как атаки на выбранный открытый текст и зашифрованный текст работают для бинарных квазигрупп.

Сначала проводились атаки, осуществляемые с использованием выбранного шифротекста.

Предположим, что криптоаналитик имеет доступ к устройству дешифрования, загруженному ключом. Затем он может построить следующий зашифрованный текст:

$$q_1q_1q_1q_2q_1q_3 \dots q_1q_n$$
$$q_2q_1q_2q_2q_2q_3 \dots q_2q_n \dots$$
$$q_nq_1q_nq_2q_nq_3 \dots q_nq_n,$$

и ввести его в дешифровальное устройство.

Устройство дешифрования выдает следующий открытый текст:

$$l\backslash q_1q_1\backslash q_1q_1\backslash q_1q_1\backslash q_1q_2\backslash q_1q_1\backslash q_3 \dots q_1\backslash q_n$$
$$q_n\backslash q_2q_2\backslash q_1q_1\backslash q_2q_2\backslash q_2q_2\backslash q_2q_2\backslash q_3 \dots q_2\backslash q_n \dots$$
$$q_n\backslash q_nq_n\backslash q_1q_1\backslash q_nq_n\backslash q_2q_2\backslash q_nq_n\backslash q_3 \dots q_n\backslash q_n.$$

В результате таблица Кэли операции "\ "определенной на Q полностью находится и построение таблицы Кэли операции " $*$ " не вызывает затруднений. Используемый в атаке шифротекст состоит из $\boldsymbol{2n^2}$ символов.

Для полной реконструкции таблицы Кэли квазигруппы $(Q, \backslash)$ достаточно ввести только $\boldsymbol{2n^2 - 4n + 1}$ символов вместо $2n^2$. Эти атаки были названы *усеченными атаками Войводы*.

Замечание 3.1.1. Сравнивая количество символов, используемых в атаке Войводы и усеченной атаке Войводы, получаем следующее предельное соотношение:

$$\lim_{n\to\infty}\frac{2n^2}{2n^2-4n+1}=1.$$

Рассмотрим новый тип атаки, которую будем называть *модифицированной атакой*. В процедуре расшифровки используется следующий текст:

$$q_1q_1q_2q_2q_3q_3\cdots q_{n-2}q_{n-2}q_{n-1}q_{n-1}q_nq_n$$
$$q_2q_1q_3q_2q_4q_3\cdots q_{n-1}q_{n-2}q_nq_{n-1}q_1q_n$$
$$q_3q_1q_4q_2q_5q_3\cdots q_nq_{n-2}q_1q_{n-1}q_2q_n\cdots.$$

Последний символ зависит от четности порядка квазигруппы, а именно, если $n-$ нечетное число, то последней операцией будет: $q_k\backslash q_n$, где $k=\left[\frac{n}{2}\right]+1$. Если же $n-$ четное число, то последней операцией будет: $q_{\frac{n}{2}}\backslash q_n$. Представленная атака требует: $\boldsymbol{n^2-2(n-1)}$ операций "\". Главное $-$ это число не зависит от используемого лидера.

Замечание 3.1.2. Сравнивая количество символов, используемых в атаке Войводы, усеченной атаке Войводы и модифицированной атаке, имеем следующие предельные соотношения: $\lim_{n\to\infty}\frac{2n^2}{n^2-2n+2}=2$ и $\lim_{n\to\infty}\frac{2n^2-4n+1}{n^2-2n+2}=2.$

Если сравнить этот результат с результатом, полученным в Замечании 3.1.1, то видно явное преимущество модифицированной атаки.

После атак с использованием выбранного шифротекста перешли к рассмотрению атак с использованием выбранного открытого текста, которые имеют свои отличительные особенности.

Предположим, у криптоаналитика есть доступ к шифровальному устройству загруженному неизвестным ключом. В работе М. Войводы [47] для шифрования строится следующий текст:

$$q_1q_1;q_1q_2;q_1q_3;\dots q_1q_n;$$
$$q_2q_1;q_2q_2;q_2q_3;\dots q_2q_n;\dots$$
$$q_nq_1;q_nq_2;q_nq_3;\dots q_nq_n.$$

Этот текст вводится в шифровальное устройство дискретно по 2 символа. Благодаря этому вводу имеем следующий зашифрованный текст:

$$l*q_1\ \ (l*q_1)*q_1;l*q_1\ \ (l*q_1)*q_2;\dots l*q_1\ \ (l*q_1)*q_n;$$
$$l*q_2\ \ (l*q_2)*q_1;l*q_2\ \ (l*q_2)*q_2;\dots l*q_2\ \ (l*q_2)*q_n;\dots$$
$$l*q_n\ \ (l*q_n)*q_1;l*q_n\ \ (l*q_n)*q_2;\dots l*q_n\ \ (l*q_n)*q_n.$$

Открытый текст, используемый в атаке, состоит из $\boldsymbol{2n^2}$ символов разделенных на пары. Однако более короткий зашифрованный текст, состоящий из $\boldsymbol{2(n-1)^2}$ символов может быть использован (*усеченная атака М.Войводы*).

Вывод осуществляется построчно на нечетной позиции– номер строки, а на четной позиции– элемент квазигруппы $(Q, *)$. Преимущество этих атак в том, что они не зависят от используемого лидера.

Теперь рассмотрим вариант, когда символы запускаются в шифровальное устройство потоком, а именно как в случае атаки с выбранным шифротекстом:

$$q_1\ q_1\ q_1\ q_2\ q_1\ q_3 \dots q_1\ q_n$$
$$q_2\ q_1\ q_2\ q_2\ q_2\ q_3 \dots q_2\ q_n \dots$$
$$q_n q_1\ q_n q_2\ q_n q_3 \dots q_n q_n \dots .$$

Будем называть эту атаку *потоковой атакой Войводы*. В ней количество используемых символов меньше, чем в предыдущих двух атаках, но результат зависит от используемого лидера. Это недостаток потоковой атаки.

Для каждого случая можно подобрать *поточную атаку с минимальным количеством символов*, но задача эта достаточно сложная. Для квазигруппы порядка n необходимое минимальное число символов равно: $\boldsymbol{n(n-2)+2}$.

Теперь рассмотрим *модифицированную атаку с использованием выбранного открытого текста с дискретным вводом символов*:

$$q_1q_1; q_2q_2; q_3q_3; \dots q_{n-2}q_{n-2}; q_{n-1}q_{n-1}; q_nq_n;$$
$$q_2q_1; q_3q_2; q_4q_3; \dots q_{n-1}q_{n-2}; q_nq_{n-1}\ ; q_1q_n;$$
$$q_3q_1; q_4q_2; q_5q_3; \dots q_nq_{n-2}; q_1q_{n-1}; q_2q_n \dots .$$

Открытый текст, используемый в этой атаке, состоит из $\boldsymbol{2(n-1)^2}$ символов разбитых на пары. Результат модифицированной атаки совпал с результатом усеченной атаки М.Войводы. Таким образом, даже в двоичном случае при проведении атак выбранным шифртекстом или выбранным открытым текстом количество используемых символов может быть уменьшено.

Были рассмотрены модификации криптографических атак, построенных М. Войводой для квазигрупп, проведен сравнительный анализ и выявлены положительные и отрицательные стороны этих атак.

В параграфах 3.3. и 3.4. показано, как атаки на выбранный открытый текст и на выбранный зашифрованный текст работают для левой и правой квазигрупп.

Сначала рассматривались атаки, осуществляемые с использованием выбранного шифротекста. Представляем результаты этих атак.

Для полной реконструкции таблицы Кэли для левой квазигруппы$(Q,\ \backslash)$, достаточно ввести только $\boldsymbol{2n^2-2n+1}$ вместо $\boldsymbol{2n^2}$ символов. Это *усеченная атака*.

Мы предложили *модифицированную атаку*. Если мы запустим следующий текст в декодер:

$$q_1q_1q_2q_2q_3q_3\cdots q_{n-2}q_{n-2}q_{n-1}q_{n-1}q_nq_n$$
$$q_2q_1q_3q_2q_4q_3\cdots q_{n-1}q_{n-2}q_nq_{n-1}q_1q_n$$
$$q_3q_1q_4q_2q_5q_3\cdots q_nq_{n-2}q_1q_{n-1}q_2q_n\cdots,$$

последний символ зависит от четности порядка квазигруппы, а именно, если n — нечетное число, то последней операцией будет: $q_n\backslash q_k$, где $k=\left[\frac{n}{2}\right]+1$. Если же $n-$ четное число, тогда последней операцией будет: $q_n\backslash q_{\frac{n}{2}+1}$.

Представленная атака требует: $\boldsymbol{n^2-2\left(n-1-\left[\frac{n}{2}\right]\right)}$ операций ” \”. По сравнению с атакой М. Войводы количество используемых символов значительно уменьшено.

Далее были рассмотрены атаки с выбранным открытым текстом для левых квазигрупп. Открытый текст, использованный в атаке М. Войводы, состоит из $\boldsymbol{2n^2}$ символов разделенных на пары. Однако более короткий текст, состоящий из $\boldsymbol{2n^2-2n}$ символов, может быть построен. В случае дискретного ввода символов результаты усеченной атаки и модифицированной атаки совпадают. При рассмотрении потоковой атаки с выбранным открытым текстом результат зависит от используемого лидера.

Наилучший результат получается при использовании модифицированной потоковой атаки. В этой атаке количество используемых символов равно: $\boldsymbol{(n-1)n+1}$, где $n-$ порядок левой квазигруппы, используемой для шифрования.

Результаты атак с выбранным шифротекстом и выбранным открытым текстом на обобщенный шифр Марковского, основанный на правых квазигруппах, аналогичны результатам, полученным для левых квазигрупп.

Работа всех приведенных атак проиллюстрирована рядом примеров.

Четвертая глава «Криптоанализ некоторых потоковых шифров ($\boldsymbol{n}$ -арный случай)», состоящая из трех параграфов, решает задачу, связанную с криптоанализом шифров, построенных с помощью обобщенного алгоритма Марковского на основе i -

обратимых n-арных группоидов, а именно, Обобщенного алгоритма 1. Это решает задачу 2.

В параграфе 4.1 исследованы атаки выбранным шифротекстом, построенным на основе i-обратимого n-арного группоида с использованием Обобщенного Алгоритма 1. Представлены модификации этих атак. Было найдено необходимое количество символов для проведения успешной атаки выбранным шифротекстом. Для ряда случаев приведены примеры текстов минимальной длины. Сделаны выводы из всех атак и проведенных исследований. Остановимся на наиболее важных из них.

Предположим, что у криптоаналитика есть доступ к устройству дешифрования, загруженному ключом. Затем он может построить следующий зашифрованный текст, где $n-$ арность, а $m-$ порядок i-обратимого группоида:

$$\underbrace{q_1q_1\cdots q_1q_1}_{n\text{ раз}}\underbrace{q_1q_1\cdots q_1q_2}\cdots\underbrace{q_1q_m\cdots q_mq_m}$$

$$\underbrace{q_2q_1\cdots q_1q_1}\underbrace{q_2q_1\cdots q_1q_2}\cdots\underbrace{q_2q_m\cdots q_mq_m}$$

$$\underbrace{q_3q_1\cdots q_1q_1}\underbrace{q_3q_1\cdots q_1q_2}\cdots\underbrace{q_3q_m\cdots q_mq_m}\cdots,$$

и вводит его в дешифрующее устройство. Этот текст является обобщенной версией текста, использованного М. Войводой для бинарных квазигрупп.

Для полной реконструкции таблицы значений операции ${}^{(i,n+1)}f$, и, следовательно, таблицы значений операции f, достаточно подать на вход: $(\boldsymbol{n\cdot m^{n-1}+1})(\boldsymbol{m-1})$ символов.

Удалось определить длину минимального необходимого текста и для ряда случаев построить такие тексты. Например, в случае $n=m=3$ нам понадобится 56 символов для полного восстановления всех значений функции ${}^{(i,4)}f$.

В следующих атаках результат был улучшен. Ввели следующий текст в дешифратор:

$$\begin{array}{ll} q_1q_1q_1q_2q_2q_2q_3q_3q_3 & 000111222 \\ q_2q_1q_1q_3q_2q_2\ q_1q_3q_3 \quad \text{или} & 100211022 \\ q_1q_2q_1q_2q_3q_2q_3q_1q_3 & 010121202 \\ q_1q_1 & 00. \end{array}$$

На выходе получено 29 символов, которых достаточно для полного восстановления всех значений функции ${}^{(i,4)}f$. Таким образом, минимальное количество символов в модифицированной атаке будет: $\boldsymbol{m^n+(n-1)}$.

В результате проведения этих двух атак удается восстановить все значения функции дешифрования. Основной проблемой модифицированной атаки является подбор оптимальных текстов для группоидов разных степеней и порядков.

Следует отметить, что для значений функции f и обратной ей функции ${}^{(i,n+1)}f$ на следующих множествах: $\left(q_{j_1}, q_{j_2}, \dots q_{j_{i-1}}, q_i, q_{j_{i+1}}, \dots q_{j_n}\right)$, где элементы $q_{j_1}, q_{j_2}, \dots q_{j_{i-1}}, q_{j_{i+1}}, \dots q_{j_n}$ выбираются из множества $\{q_1, q_2, \dots q_m\}$ и являются фиксированными элементами, при разных значениях элемента $q_i -$ соответствующие функции не могут принимать одинаковые значения. Для каждого такого фиксированного набора достаточно определить $(m-1)$ значение соответствующей функции, и последнее значение будет найдено автоматически. С учетом этого замечания построенный текст будет иметь длину: $\boldsymbol{m^{n-1} \cdot (m-1)}$.

Следует отметить две особенности такого текста:

1) Определение значений остальных функций (их осталось m^{n-1}) является более сложной задачей, чем в случае работы с бинарными квазигруппами;

2) Для случая $n = m = 3$ такой текст найден, но можно ли будет подобрать аналогичный текст в других случаях? И можно ли будет найти общий вид такого текста, или он будет разным для каждого случая?

Например, для случая $n = m = 3$, чтобы восстановить таблицу значений операции ${}^{(i,4)}f$, достаточно ввести 20 символов (восстановим 18 значений из 27):

$$q_1q_1q_1q_2q_2q_2q_3q_3q_3 \quad 000111222$$
$$q_2q_1q_2q_1q_3q_1q_3q_2q_3 \quad \text{или} \quad 101020212$$
$$q_1q_2 \quad 01.$$

Этот текст имеет наименьшую длину для случая $n = m = 3$. Особенность этой атаки в том, что мы получаем не все значения функции, а лишь достаточное количество символов для восстановления всей таблицы.

Предположим теперь, что ключ взломан и нам нужно взломать расшифрованный текст. Ситуация будет следующей: первые $(n-1)$ символов, содержащие лидеров, могут принимать любые значения, а все остальные символы будут определяться ими. Поэтому возможных вариантов дешифрируемых текстов будет: $\boldsymbol{m^n}$.

В параграфе 4.2. мы рассмотрели атаки выбранным открытым текстом, построенным с использованием n-арных группоидов, которые обратимы на i-м месте, полученным с

помощью Обобщенного Алгоритма 1. Особенностью таких атак является то, что для них невозможно подобрать оптимальный вариант общего текста.

Предположим, что у криптоаналитика есть доступ к шифровальному устройству, загруженному ключом. Он может построить следующий открытый текст ($n-$ это арность операции, $m-$ порядок i-обратимого группоида):

$$\underbrace{q_1q_1\dots q_1q_1}_{n\text{ раз}}\underbrace{q_1q_1\dots q_1q_2}\dots\underbrace{q_1q_1\dots q_1q_m}$$

$$\underbrace{q_1q_1\dots q_2q_1}\underbrace{q_1q_1\dots q_2q_2}\dots\underbrace{q_1q_1\dots q_2q_m}$$

$$\underbrace{q_1q_1\dots q_3q_1}\underbrace{q_1q_1\dots q_3q_2}\dots\underbrace{q_1q_1\dots q_3q_m}\dots$$

$$\underbrace{q_1q_1\dots q_mq_1}\underbrace{q_1q_1\dots q_mq_2}\dots\underbrace{q_1q_1\dots q_mq_m}\dots,$$

и вводит его в шифровальное устройство.

Количество символов, необходимых для восстановления таблицы шифрования, зависит от значений выбранных лидеров. Поэтому вопрос определения длины используемого открытого текста в каждом случае решается индивидуально. Работа данного вида атаки иллюстрируется рядом примеров.

В заключение хотелось бы сказать несколько слов о криптоанализе шифров, построенных на основе Обобщенного Алгоритма 2. Этот криптоанализ представляет собой очень сложную задачу, в связи с тем, что отсутствует какая-либо информация о степенях трансляций, используемых в алгоритме. Это еще раз указывает на то, что Обобщенный Алгоритм 2 более устойчив к криптоанализу, чем Обобщенный Алгоритм 1.

Учитывая проведенное исследование, можно сделать вывод, что оба обобщенных алгоритма представляют большой интерес для использования в криптографии.

3. ОБЩИЕ ВЫВОДЫ И РЕКОМЕНДАЦИИ

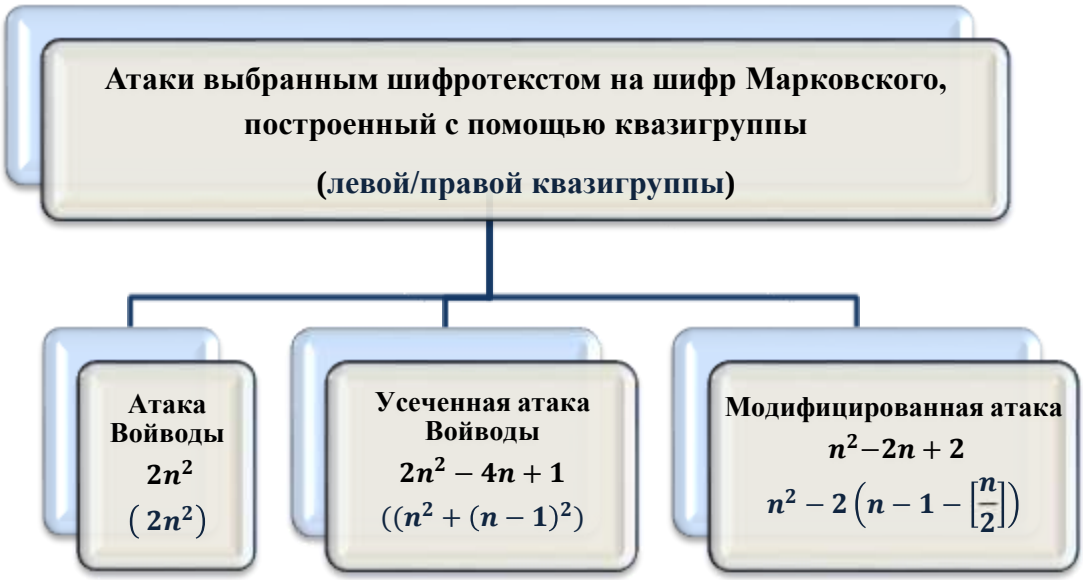
Исследование, выполненное в рамках докторской диссертации «**Использование информационных технологий в разработке криптографических и алгебраических алгоритмов**», полностью соответствует цели и задачам, изложенным во вводной главе.

Результаты работы являются новыми и оригинальными. Разработаны и обобщены алгоритмы, позволившие улучшить работу классического алгоритма Марковского; изучены атаки на построенные шифры и показана степень стойкости этих шифров.

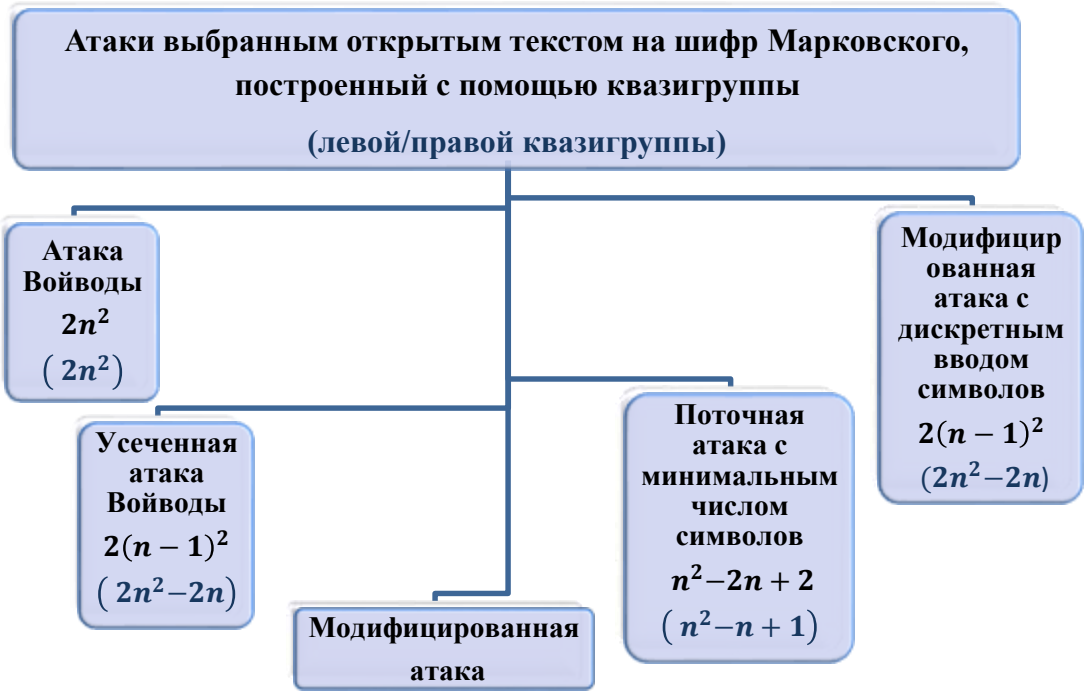
Теоретическая значимость диссертации определяется получением новых алгоритмов и шифров, построенных с использованием неассоциативных структур, таких как n-арные группоиды и квазигруппы. Прикладное значение диссертации заключается в использовании полученных результатов в теории кодирования и криптоанализе.

Анализируя полученные результаты, можно сделать следующие общие выводы:

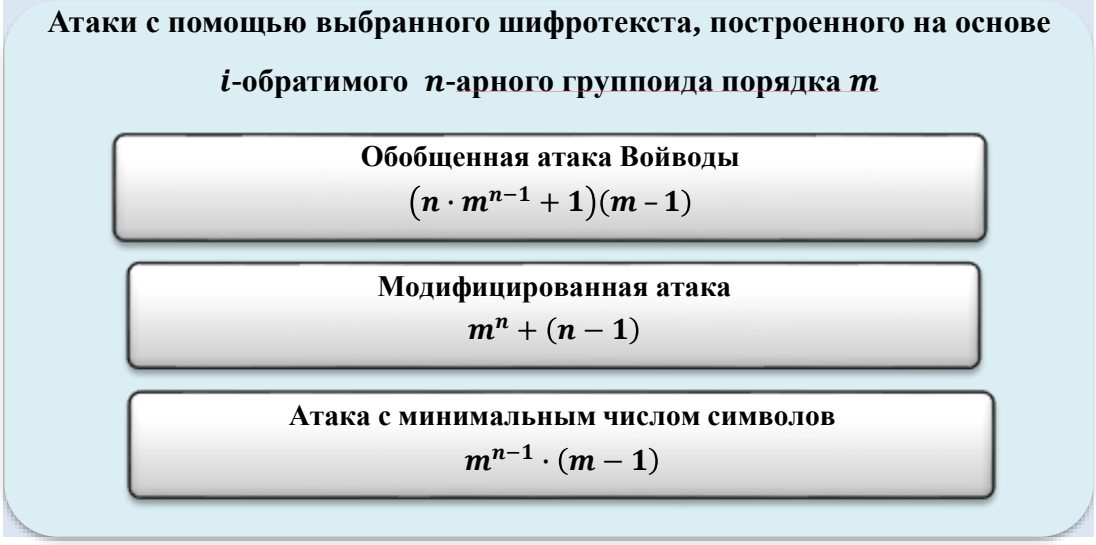
1. Ключевой задачей защиты информации является создание надежных алгоритмов шифрования, поэтому любой вновь построенный алгоритм необходимо подвергать тщательному анализу с целью выявления его слабых мест и возможности взлома.
2. Использование квазигрупп в криптологии показывает лучшие возможности и результаты, чем использование ассоциативных систем.
3. Разработаны обобщенные алгоритмы Марковского для левой и правой квазигрупп и программы для их реализации, которые имеют свои особенности и преимущества.
4. Проведены атаки выбранным шифротекстом на шифры Марковского, построенные с использованием квазигрупп (левых и правых квазигрупп), проведен сравнительный анализ этих атак и предложены новые модифицированные атаки с улучшенными результатами. Отобраны тексты минимальной длины для каждой построенной атаки.



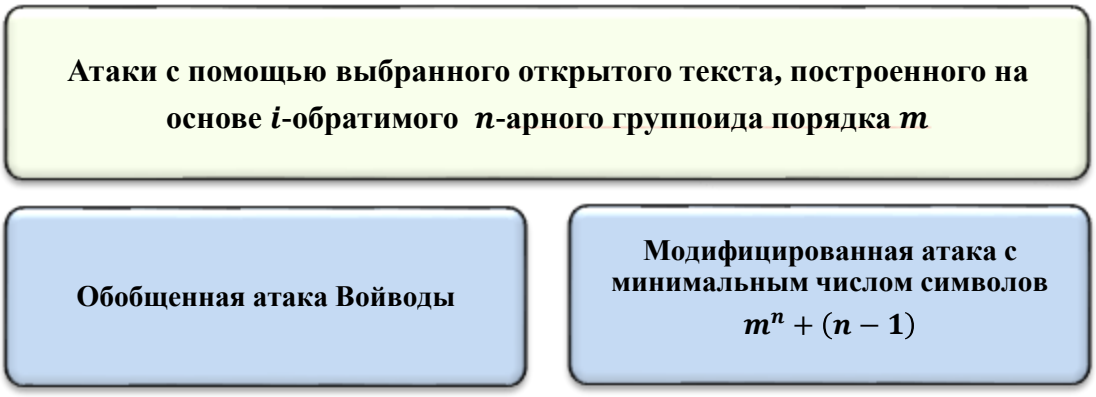
5. Проведены атаки выбранным открытым текстом на шифры Марковского, построенные с использованием квазигрупп, выявлены положительные и отрицательные стороны этих атак и предложены новые модифицированные атаки. Для потоковых атак выбранным открытым текстом определяется минимальное необходимое количество символов для полного восстановления таблицы квазигруппы шифрования (текст зависит от используемого лидера).



6. Построен обобщенный алгоритм Марковского для n-арного группоида, обратимого на одном фиксированном месте – Обобщенный Алгоритм 1 и разработаны программы, реализующие работу этого алгоритма.
7. Описаны атаки с использованием выбранного шифротекста на шифр, полученный с помощью обобщенного алгоритма Марковского (Обобщенного Алгоритма 1).



8. Атака на шифротекст может быть осуществлена путем полного перебора всех значений функций, в которых фигурируют лидеры. Общее количество этих значений равно m^{n-1}.
9. Описаны атаки с использованием выбранного открытого текста на шифр, полученный с помощью обобщенного алгоритма Марковского (Обобщенного Алгоритма 1).



10. Для группоидов третьего и четвертого порядка построены тексты наименьшей длины, но в каждом случае они подбираются индивидуально. Подбор такого текста – сложная задача.

11. Построен обобщенный алгоритм Марковского для n -арного группоида, обратимого на одном фиксированном месте, с использованием трансляций любых степеней – Обобщенный Алгоритм 2 и написаны программы, реализующие работу этого алгоритма.
12. Общее количество необходимых лидеров для первого алгоритма будет равно: $(\boldsymbol{n-1})^{\boldsymbol{2}}$. Для второго алгоритма необходимое количество лидеров будет равно: $\frac{(\boldsymbol{n-1})\boldsymbol{n}}{\boldsymbol{2}}$. Второе число меньше первого на величину: $(\boldsymbol{n-1})\left(\frac{\boldsymbol{n}}{\boldsymbol{2}}-\boldsymbol{1}\right)$. Это говорит о преимуществе второго алгоритма перед первым (особенно с ростом числа n).
13. Обобщенный Алгоритм 2 будет значительно сложнее, если помимо первой и второй степени трансляций будут использоваться третья, четвертая и другие степени. Особый интерес представляет определение обратных трансляций для тех, которые используются в Обобщенном Алгоритме 2.
14. Проведен анализ всех разработанных программ, который включает в себя оценку наиболее важных параметров (среди них: длина текста, используемый алгоритм, количество необходимых лидеров, средняя скорость обработки данных, оценка сложности алгоритма с помощью концепции Big-O). В результате был сделан вывод, что программы работают успешно и имеют положительные характеристики.
15. Рассмотрен аналог системы шифрования Эль-Гамаля на основе алгоритма Марковского и изучены его особенности. Для него планируются новые модификации. Криптоанализ этой обобщенной схемы представляет собой сложную задачу, требующую решения.

Предлагаемые разработки имеют весомую научную ценность в связи с их высокой степенью новизны и оригинальности. Полученные в работе результаты имеют теоретическую и прикладную ценность в таких областях, как алгебра, криптология и информатика.

Рекомендации:

1. Особый интерес представляет продолжение применения алгоритма Марковского в теории кодирования и особенно в криптографии.
2. Исследования по тематике диссертации могут быть продолжены как с алгебраической, так и с прикладной точек зрения. Особо важным является исследование возможностей использования квазигрупп и других неассоциативных систем в криптологии и теории кодирования.
3. Построенные алгоритмы могут быть использованы в банковских информационных системах, а также при разработке различных банковских продуктов, как дополнительная защита, повышающая надежность и долговечность данных систем и продуктов (например, в современных пластиковых картах).
4. Полученные результаты могут быть использованы для разработки алгебраических и криптографических алгоритмов в различных областях информатики.
5. Содержание диссертации может служить основой для разработки спецкурсов для докторантов и магистрантов.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

[1]MAGLIVERAS, STINSON, VAN TRUNG, T. New Approaches to Designing Public Key Cryptosystems Using One-Way Functions and Trapdoors in Finite Groups. In: *J. Cryptology*. 2002, vol.15, no.4, pp. 285-297. ISSN 1432-1378.

[2]DEHORNOY, P. Braid-based cryptography. In: *Contemporary Mathematics, Group Theory, Statistics, and Cryptography*. 2004, vol. 360, pp. 5-33. ISBN 978-0-8218-3444-2.

[3]DENES, J., KEEDWELL, A. D. Some applications of non-associative algebraic systems in cryptology. In: *Pure Mathematics and Applications*. 2001, vol. 12(2), pp.147-195. ISSN 1218-4586.

[4]KOSCIELNY, Cz. $NLPN$ Sequences over $GF(q)$. In: *Quasigroups and Related Systems*. 1997, vol.4, no.1, pp. 89-102. ISSN 1561-2848.

[5]DENES, J., KEEDWELL, A. D. Latin Squares and their Applications. In: *Bulletin of the American mathematical society*. 1976, vol.82, no.3, pp. 468-471. ISSN 0273-0979.

[6]DENES, J., KEEDWELL, A.D. Latin squares: New Developments in the Theory and Applications. In: *Annals of Discrete mathematics*. 1991, North-Holland, vol. 46, pp. 1-469. ISSN 0167-5060. ISBN 0 444 88899 3.

[7]DENES, J. On Latin squares and a digital encrypting communication system. In: *P.U.M.A., Pure Mathematics and Applications*, Department of Mathematics, Corvinus University of Budapest. 2000, vol. 11, iss.4, pp.559-563. ISSN 1218-4586.

[8]KALKA, A. *Non-associative public-key cryptography*. 2012. 32 p. [Online]. Available: https://arxiv.org/pdf/1210.8270.pdf

[9]ТУЖИЛИН, М. Э. Латинские квадраты и их применение в криптографии. В: *Прикладная дискретная математика, Математические методы криптографии*. 2012, №3(17), с. 47-52. ISSN 2311-2263 (Online).

[10] МОВСИСЯН, Ю. Сверхтождества в алгебрах и многообразиях. В: *Успехи математических наук*. 1998, том 53, выпуск 1(319), с. 61-114. ISSN 0042-1316.

[11] ГРИБОВ, А.В., ЗОЛОТЫХ, П.А., МИХАЛЕВ, А.В. Построение алгебраической криптосистемы над квазигрупповым кольцом. В: *Математические вопросы криптографии*. 2010, том 1, выпуск 4, с. 23-32. ISSN 2220-2617.

[12] MAZE, G., MONICO, C., ROSENTHAL, J. Public key cryptography based on semigroup actions. In: *Advances in Mathematics of Communications*. 2007, vol.1, no.4, pp.489-507. ISSN 1930-5346.

[13] SHPILRAIN, V., USHAKOV, A. Thompson's Group and Public Key Cryptography. In: *Applied Cryptography and Network Security*, ACNS, Lecture Notes in Computer Science, Springer. 2005, vol. 3531, pp.151-163. ISBN 978-3-540-26223-7. ISSN 0302-9743.

[14] ATANI, R.E., ATANI, SH.E., MIRZAKUCHAKI, S. Public Key Cryptography Based on Semimodules over Quotient Semirings. In: *International Mathematical Forum*. 2007, vol.2, no.52, pp.2561-2570. ISSN 1312-7594.

[15] KRAPEZ, A. Cryptographically Suitable Quasigroups via Functional Equations. In: *ICT Innovations 2012*, Advances in Intelligent Systems and Computing. 2013, vol. 207, pp. 265-274. ISSN 1857-7288.

[16] KRAPEZ, A. ŠEŠELJA, B., TEPAVČEVIĆ, A. Solving linear equations by fuzzy quasigroups techniques. In: *Information Sciences*. 2019, vol. 491, pp.179-189. ISSN 0020-0255.

[17] MEYER, K. A. *A New Message Authentication Code Based on the Non-Associativity of Quasigroups*: PhD thesis of doctor of philosophy. Iowa State University, 2006. 91 p.

[18] ARTAMONOV, V. Applications of quasigroups to cryprography. In: *Sarajevo Journal of Mathematics.* 2018, vol.14 (27), no.2, pp. 191–205. ISSN 1840-0655.

[19] ARTAMONOV, V., CHAKRABARTI, S., MARKOV, V., PAL, S. Constructions of polynomially complete quasigroups of arbitrary order. In: *Journal of Algebra and Its Applications.* 2020, vol.20, no.12, 2150236. ISSN 0219-4988.

[20] KOSCIELNY, Cz., MULLEN, G.L. A quasigroup-based public-key cryptosystem. In: *International Journal of Applied Mathematics and Computer Science*. 1999, vol.9, no.4, pp. 955-963. ISSN 1641-876X.

[21] OCHODKOVA, E., SNASEL, V. Using quasigroups for secure encoding of file system. In: *Proceedings of the Conference Security and Protection of Information*, Abstract of Talks, Military Academy in Brno. 2001, pp. 175-181. ISBN 8085960281.

[22] MARKOVSKI, S., GLIGOROSKI, D., STOJCEVSKA, B. Secure two-way on-line communication by using quasigroup enciphering with almost public key. In: *Novi Sad Journal of Mathematics*. 2000, vol. 30, iss.2, pp. 43-49. ISSN 0352-0900.

[23] MARKOVSKI, S., GLIGOROSKI, D., BAKEVA, V. Quasigroup string processing: Part 1. In: *Proc. of Maked. Academ. of Sci. and Arts for Math. and Tech. Sci*. XX (1-2). 1999, pp.13-28. ISSN 1857-9027.

[24] MARKOVSKI, S., DIMITROVA, V., TRAJCHESKA, Z., PETKOVSKA, M., KOSTADINOSKI, M., BUHOV, D. Block cipher defined by matrix presentation of quasigroups. In: *IACR Cryptology ePrint Archive*. 2021, vol. 2021/ 1512, 3 p.

[25] SHCHERBACOV, V.A. *Elements of Quasigroup Theory and Applications*. 1st ed: Chapman and Hall/CRC, 2017. 598 p. ISBN 9781315120058.

[26] BAKEVA, V., DIMITROVA, V. Some probabilistic properties of quasigroup processed strings useful in cryptanalysis. In: *Communications in Computer and Information Science*. 2011, vol.83, pp. 61-70. ISSN 1865-0929.

[27] BAKEVA, V., DIMITROVA, V., POPOVSKA-MITROVIKJ, A. Parastrophic quasigroup string processing. In: *Proceedings of the 8th Conference on Informatics and Information Technologies with International Participation*, 2011, Bitola, Macedonia, pp.19-21.

[28] DIMITROVA, V., BAKEVA, V., POPOVSKA-MITROVIKJ, A., KRAPEZ, A. Classifications of quasigroups of order 4 by parastrophic quasigroups tranformation. In: *The International Mathematical Conference on Quasigroups and Loops, LOOPS'11*, Booklet of Abstracts, Trest, Czech Republic, 2011, p.6.

[29] KRAPEZ, A., ZIVKOVIC, D. Parastrophically equivalent quasigroup equations. In: *Publications de l'Institut Mathématique*, Nouvelle Série, Beograd. 2010, vol.87(101), pp.39-58. ISSN 0350-1302.

[30] VOJVODA, M. *Stream Ciphers and Hash Functions: Analysis of Some New Design Approaches*: PhD thesis in technical sciences. Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology, Bratislava, Slovak Republic, 2004. 94 p

[31] SHCHERBACOV, V.A., *Elements of quasigroup theory and some its applications in code theory and cryptology*, 2003. 85 p. [online]. Available: https://www2.karlin.mff.cuni.cz/~drapal/speccurs.pdf

[32] SHCHERBACOV, V.A. *On some known possible applications of quasigroups in cryptology*, 2003. 15 p. [online]. Available: https://www2.karlin.mff.cuni.cz/~drapal/krypto.pdf

[33] PETRESCU, A. Applications of quasigroups in cryptography. In: *Interdisciplinarity in Engineering Scientific International Conference Tg. Mures*-Romania, 15-16 November, 2007, 5 p. ISSN 2285-0945.

[34] PETRESCU, A. n-Quasigroup cryptographic primitives: Stream ciphers. In: *Studia Universitatis Babeş-Bolyai Informatica*. 2010, vol. LV, iss.2, pp. 27-34. ISSN 1224-869X.

[35] SHCHERBACOV, V.A. Quasigroups in cryptology. In: *Computer Science Journal of Moldova*. 2009, vol.17, no.2(50), pp. 193-228. ISSN 1561-4042.

[36] GLIGOROSKI, D., MARKOVSKI, S., KOCAREV, L. Edon-R, an infinite family of cryptographic hash functions. In: *International Journal of Network Security*. 2009, vol.8, no.3, pp.293-300. ISSN 1816-353X.

[37] GLIGOROSKI, D., MARKOVSKI, S., KNAPSKOG, S. J. *A public key block cipher based on multivariate quadratic quasigroups*, 2008. 22 p. [Online]. https://arxiv.org/abs/0808.0247

[38] HASSINEN, M., MARKOVSKI, S. Secure SMS messaging using Quasigroup encryption and Java SMS API. In: *Proceedings of the Eighth Symposium on Programming Languages and Software Tools SPLST'03*, June 17-18, 2003, Kuopio, Finland, pp.187-200.

[39] CHAKRABARTI, S., SAIBAL, K. P., SUGATA, G. An Improved 3-Quasigroup based Encryption Scheme. In: *ICT Innovations 2012, Secure and Intelligent Systems*, Web Proceedings, 2012, Ohrid, Macedonia, pp.173-184. ISSN 1857-7288.

[40] CSORGO, P., SHCHERBACOV, V. *On some quasigroup cryptographical primitives*, 2011. 11 p. [online]. https://arxiv.org/abs/1110.6591

[41] MOLDOVYAN, N.A., SHCHERBACOV, A.V., SHCHERBACOV, V.A. On some applications of quasigroups in cryptology. In: *Proceedings of the Workshop on Foundations of Informatics FOI-2015*, August 24-29, 2015, Chisinau, Republic of Moldova. pp.331-341. ISBN 978-9975-4237-3-1.

[42] ГРИБОВ, А.В. *Алгебраические неассоциативные структуры и их приложения в криптологии*: кандидатская диссертация, кандидата физико-математических наук, МГУ, Москва, 2015. 93 с.

[43] БЕЛОУСОВ, В.Д. *n-арные квазигруппы*. Кишинев: Штиинца, 1972. 225 с.

[44] ELGAMAL, T. A public key cryptosystem and a signature scheme based on discrete logarithms. In: *IEEE Transactions on Information Theory*. 1985, vol.31, no.4, pp. 469-472. ISSN 0018-9448.

[45] SHCHERBACOV, V.A. On the structure of left and right F-, SM- and E-quasigroups. In: *Journal of Generalized Lie Theory and Applications*. 2009, vol. 3, no.3, pp.197-259. ISSN 1736-5279.

[46] VOJVODA, M. Cryptanalysis of a file encoding system based on quasigroup. In: *Journal of Electrical Engineering*. 2003, vol.54, no.12. ISSN 1335-3632.

[47] VOJVODA, M. *Attacks on a file encryption system based on quasigroup*. In: *Proceedings of Elitech 2003*, Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology,2003, Bratislava, Slovak Republic, pp. 54-56.

АННОТАЦИЯ

Малютина Надежда: "Использование информационных технологий в разработке криптографических и алгебраических алгоритмов"

Докторская диссертация по информатике, Кишинёв, 2023

Структура диссертации: диссертация состоит из введения, четырех глав, общих выводов и рекомендаций, списка литературы из 201 источника и 3 приложений. Диссертация содержит 145 страниц основного текста, 1 рисунок и 71 таблицу. Полученные результаты были опубликованы в 21 научной работе.

Ключевые слова: Алгоритм Марковского, квазигруппа, левая и правая квазигруппа, трансляция, открытый текст, зашифрованный текст, атака, ключ, шифрование, дешифрование.

Цель исследования: построение новых и усовершенствование уже построенных криптографических алгоритмов и их криптоанализ.

Задачи исследования: 1. Разработка эффективного криптографического алгоритма на основе алгоритма Марковского с использованием n-арных группоидов; 2. Написание программ, реализующих работу построенных алгоритмов; 3. Проведение атак на все построенные шифры; 4. Сравнительный анализ проведенных атак; 5. Нахождение текстов минимальной длины для всех исследованных типов атак.

Научная новизна и оригинальность работы: результаты работы новые и оригинальные. Они являются продолжением предыдущих исследований в этой области. Разработаны и обобщены алгоритмы, которые позволили улучшить работу классического алгоритма Марковского, изучены атаки на построенные шифры и показана степень стойкости этих шифров.

Полученный результат, который способствует решению важной научной проблемы: состоит в разработке новых обобщений классического алгоритма, которые способствуют увеличению стойкости построенного шифра к известным видам атак.

Теоретическая значимость работы: определяется получением новых алгоритмов и шифров, построенных с применением неассоциативных структур, таких как n-арные группоиды. Разработаны новые обобщения алгоритмов кодирования с использованием левых и правых квазигрупп, n-арных группоидов обратимых на одном фиксированном месте.

Прикладная ценность работы заключается в использовании полученных результатов в теории кодирования и криптоанализе.

Внедрение научных результатов: Полученные результаты могут быть использованы в научных исследованиях, связанных с кодированием данных, изучением эффективности представления информации, криптоанализе данных. Они также могут быть использованы при разработке факультативного курса для студентов университетов, связанного с изучением криптологии на абстрактных алгебраических структурах.

ADNOTARE

Maliutina Nadejda: "Utilizarea tehnologiilor informaționale la elaborarea algoritmilor criptografici și algebrici"

Teză de doctor în informatică, Chișinău, 2023

Structura tezei: teza constă din introducere, patru capitole, concluzii generale și recomandări, bibliografie din 201 titluri și 3 anexe. Teza conține 145 pagini de text de bază, o figură și 71 tabele. Rezultatele obținute sunt publicate în 21 lucrări ştiințifice.

Cuvinte-cheie: algoritm Markovski, cvazigrup, cvazigrup de stânga și de dreapta, translație, text deschis, text cifrat, atac, cheie, criptare, decriptare.

Scopul lucrării: construirea noilor și îmbunătățirea algoritmilor criptografici deja construiți și a criptoanalizei acestora.

Obiectivele cercetării: 1. Dezvoltarea unui algoritm criptografic eficient bazat pe algoritmul Markovski folosind grupoizi n-ari; 2. Elaborarea programelor, care implementează lucrul algoritmi construiti; 3. Efectuarea atacurilor asupra tuturor cifrurilor construite; 4. Analiza comparativă a atacurilor comise; 5. Găsirea textelor de lungime minimă pentru toate tipurile de atacuri investigate.

Noutatea și originalitatea științifică: Rezultatele lucrării sunt noi și originale. Ele sunt o continuare a cercetărilor anterioare în acest domeniu. Au fost dezvoltați și generalizați algoritmi, care au permis îmbunătățirea activității algoritmului clasic Markovski, au fost studiate atacurile asupra cifrurilor construite și a fost arătat gradul de rezistență al acestor cifruri.

Rezultatul obținut care contribuie la soluționarea unei probleme ştiinţifice importante: constă în dezvoltarea noilor generalizări ale algoritmului clasic care cresc rezistența cifrului construit la tipuri cunoscute de atacuri.

Semnificația teoretică a lucrării: este determinată prin obținerea noilor algoritmi și cifrurilor construite, folosind structuri neasociative precum grupoizii n-ari. Sunt dezvoltate noi generalizări ale algoritmilor de codare folosind cvazigrupuri de stânga și de dreapta, grupoizi n-ari inversabili la un loc fixat.

Valoarea aplicativă: constă în utilizarea rezultatelor obținute în teoria codificării și criptoanaliză.

Implementarea rezultatelor ştiinţifice: rezultatele obținute pot fi utilizate în cercetările științifice legate de codificarea datelor, studierea eficienței prezentării informațiilor și criptoanaliza datelor. Ele pot fi utilizate și în proiectarea unui curs opțional pentru studenții universitari legat de studiul criptologiei pe structuri algebrice abstracte.

ANNOTATION

Malyutina Nadezhda: "The use of information technologies in the development of cryptographic and algebraic algorithms"

PhD Thesis in Computer Science, Chisinau, 2023

Thesis structure: the thesis consists of Introduction, four main chapters, general conclusions and recommendations, bibliography of 201 sources, and 3 annexes. The thesis contains 145 pages of the main text, one figure, and 71 tables. The obtained results were published in 21 scientific works.

Keywords: Markovski algorithm, quasigroup, left and right quasigroup, translation, plaintext, ciphertext, attack, key, encryption, decryption.

The purpose of the thesis: construction of new modifications and improvement of already developed cryptographic algorithms and their cryptanalysis.

The objectives of the work: 1. Development of an effective cryptographic algorithm based on the Markovski algorithm using n-ary groupoids; 2. Writing programs that perform the work of the constructed algorithms; 3. Carrying out attacks on all built ciphers; 4. Comparative analysis of the attacks carried out; 5. Finding texts of the minimum length for all investigated types of attacks.

The scientific novelty and originality: the main results of the work are new and original. They are a continuation of previous research in this area. Algorithms were developed and generalized that allowed us improving the work of the classical Markovski algorithm, the attacks on the constructed ciphers were studied, and the degree of resistance of these ciphers was shown.

The important scientific problem being solved in the research: it consists in the development of new generalizations of the classical algorithm, which contribute to an increase in the resistance of the constructed cipher to known types of attacks.

The theoretical significance of the thesis: is determined by obtaining new algorithms and ciphers built using non-associative structures such as n-ary groupoids. New generalizations of coding algorithms using left and right quasigroups, n-ary groupoids invertible in one fixed place are developed.

The applicative value of the thesis: it lies in the use of the obtained results in coding theory and cryptanalysis.

The implementation of the scientific results: the results obtained can be used in scientific research related to data coding, study of the efficiency of information presentation, and data cryptanalysis. They can also be used in the design of an elective course for university students related to the study of cryptology on abstract algebraic structures.

UNIVERSITATEA DE STAT DIN MOLDOVA

ŞCOALA DOCTORALĂ ȘTIINȚE FIZICE, MATEMATICE, ALE INFORMAȚIEI ȘI INGINEREȘTI

Cu titlu de manuscris

C.Z.U: 519.21:004.421(043.2)

MALIUTINA NADEJDA

UTILIZAREA TEHNOLOGIILOR INFORMAȚIONALE LA ELABORAREA ALGORITMILOR CRIPTOGRAFICI ȘI ALGEBRICI

Rezumatul tezei de doctor în informatică

122.03 – Modelare, metode matematice, produse program

Autor: Maliutina Nadejda

Conducători ştiinţifici: Corlat Andrei, dr. în şt. fizico-matematice, prof. univ.

Şcerbacov Victor, dr. hab. în şt. fizico-matematice, prof. univ.

Comisia de îndrumare: Arnautov Vladimir, dr. hab. în şt. fizico-matematice, acad.

Cojocaru Svetlana, dr. hab. în informatică, m.cor., prof. cerc.

Ţiţchiev Inga, dr. în informatică, conf. univ.

CHIŞINĂU, 2023

Малютина, Надежда

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАЗРАБОТКЕ КРИПТОГРАФИЧЕСКИХ И АЛГЕБРАИЧЕСКИХ АЛГОРИТМОВ

122.03 – МОДЕЛИ, МАТЕМАТИЧЕСКИЕ МЕТОДЫ, ПРОГРАММНЫЕ ПРОДУКТЫ

Автореферат докторской диссертации по информатике

Подписано в печать: 09.03.2023	Размер бумаги 60x84 1/16
Бумага офсетная.	Тираж 30 экз.
Печать листов: 1,5	Заказ 15

Магазин «ПРИНТЕР», ул. Свердлова, 92, г.Тирасполь, MD-3300

Email: alex@impreso.md