а также чуть больше время чтения), которые пока не позволяют стать ей на первое место среди других *RAM*. Но стоит отметить, что сегнетоэлектрическая память стремительно развивается и в скором будущем может стать одним из востребованных и коммерциализированных типов энергонезависимой памяти [4; 5].

Заключение. В результате проведенного исследования был рассмотрен принцип работы ЭЗУ на основе сегнетоэлектриков, проведён анализ и сравнение *FRAM*-памяти с другими видами *RAM*-памяти и было установлено, что некоторые недостатки и конкуренция с другими технологиями запоминающих устройств на данный момент ограничивает ее популярность на рынке, но при должном развитии *FRAM* может стать одним из ведущих видов ЭЗУ.

1. Сегнетоэлектрики. Характеристики сегнетоэлектриков. – URL: https://www.booksite.ru/fulltext/1/001/008/100/712.htm (дата обращения: 07.03.2024).

2. Фазовые переходы в сегнетоэлектриках с распределенной поляризацией, вызванной закономерным изменением состава: Договор с БРФФИ №№ Ф08Р-110 от 1 апр. 2008 г. : отчет о НИР (заключ.) / науч. рук. В. Н. Шут ; [исполн.: В. Н. Шут, И. Ф. Кашевич, С. Е. Мозжаров, Ю. А. Шиенок]; М-во образования Республики Беларусь, УО "ВГУ им. П. М. Машерова". – Витебск, 2010. – 46 л. – URL: https://rep.vsu.by/handle/123456789/24873 (дата обращения: 07.03.2024).

3. Перспективные технологии производства памяти. Современное состояние. – URL: https://kit-e.ru/perspektivnye-tehnologii-proizvodstva-pamyati-sovremennoe-sostoyanie/ (дата обращения: 07.03.2024).

4. Перспективные виды памяти с произвольным доступом и новые уязвимости СВТ на их основе. – URL: https://bit.mephi.ru/index.php/bit/article/viewFile/169/175 (дата обращения: 07.03.2024).

5. Другие перспективные виды памяти. – URL: https://itelon.ru/blog/drugie-perspektivnye-vidy-pamyati-chast-2/ (дата обращения: 07.03.2024).

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ КОМПЬЮТЕРНОЙ АЛГЕБРЫ GAP ДЛЯ ОПРЕДЕЛЕНИЯ КОЛИЧЕСТВА АТОМОВ РЕШЁТКИ ПОДГРУПП

Столяренко А.Ю.,
магистрант 2 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – Мехович А.П., канд. физ.-мат. наук

GAP (Groups, Algorithms and Programming) является системой компьютерной алгебры, задуманной как инструмент вычислительной теории групп, и впоследствии распространившейся на смежные разделы алгебры [1].

Использование системы компьютерной алгебры при изучении теории групп позволяет упростить работу со сложными математическими объектами, такими как группы, подгруппы, решётки, облегчить их изучение и понимание. Система компьютерной алгебры GAP успешно используется при выявлении и анализе структурных характеристик, установлении взаимосвязей между изучаемыми объектами.

Актуальность работы подтверждается тем, что она представляет собой способ определения количества атомов в решётках подгрупп с использованием системы компьютерной алгебры GAP.

Целью настоящей работы является описание реализованного алгоритма отыскания количества атомов решётки подгрупп посредствам системы компьютерной алгебры GAP.

Материал и методы. В работе используется терминология и методы исследования конечных групп и их решеток, а также вычислительные методы системы компьютерной алгебры GAP.

Результаты и их обсуждение. В определениях и обозначениях следуем стандартной терминологии теории групп и их классов, а также теории решеток. Все необходимые термины можно найти в [2–5].

Напомним, что решёткой называется частично упорядоченное множество, в котором каждое двухэлементное подмножество обладает как точной верхней, так и точной нижней гранью [4].

Наименьший элемент в решётке обозначается 0 (нуль, нулевой элемент) [5].

Элемент a решётки L с нулём называется атомом, если для любого $x \in L$ из $0 < x \leq a$ следует, что $x = a$ (т. е. если элемент a покрывает нуль решётки L) [3].

Алгоритм поиска количества атомов решётки подгрупп основан на проверке всех элементов решётки, удовлетворяющих определению атома решётки.

В алгоритме определена вспомогательная рекурсивная функция EqualOrCovers(x, y, G), реализующая проверку существования отношения покрытия между элементами x и y заданной решётки подгрупп группы G.

Основная функция алгоритма GroupAtoms(G) проверяет элементы решётки подгрупп группы G на соответствие определению атома решётки. Для корректного определения и подсчёта количества атомов, создаются переменные для хранения информации о подгруппах группы G, значении счётчика атомов, элементах решётки.

С помощью циклов, проходящих по всем парам элементов решётки подгрупп и проверяющих для них выполнение определения атома решётки, заполняется список элементов-атомов. Если для элемента решётки выполнились необходимые условия определения атома решётки, счётчик количества атомов увеличивается на единицу, в противном случае, цикл прерывается. Действия повторяются для следующей пары элементов.

Результатом работы программы является количество найденных атомов решётки подгрупп.

Заключение. В работе описан реализованный алгоритм определения количества атомов решётки подгрупп посредствам системы компьютерной алгебры GAP.

1. GAP System for Computational Discrete Algebra [Электронный ресурс]. – URL: https://www.gap-system.org/ (дата обращения: 10.03.2024).

2. Биркгоф, Г. Теория решеток: пер. с англ. / К. Биркгоф. – М.: Наука. Главная редакция физико-математической литературы, 1984. – 568 с.

3. Владимиров, Д.А. Булевы алгебры / Д.А. Владимиров. – М.: Наука, 1969. – 320 с.

4. Салий, В. Н. Решетки с единственными дополнениями / В. Н. Салий // М : Наука. Главная редакция физико-математической литературы, 1984 г. – 128 с.

5. Вечтомов, Е. М. Практикум по теории упорядоченных множеств и решёток / Е. М. Вечтомов // Математический вестник педвузов и университетов Волго-Вятского региона. – 2018. – вып. 3. – С. 4–17.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ И ЕЁ РЕАЛИЗАЦИЯ НА ОСНОВЕ ЗАДАЧИ О РЮКЗАКЕ

Федорченко Т.Е.,

студент 1 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь

Научный руководитель – Ермоченко С.А., канд. физ.-мат. наук, доцент

Внедрение криптографической системы, основанной на задаче о рюкзаке [1], в производственные процессы может быть использовано для обеспечения защиты конфиденциальной информации и противодействию потенциальным угрозам кибербезопасности. Этим объясняется актуальность темы данного исследования. Задача о рюкзаке предусматривает формирование подмножества объектов заданного множества при имеющемся наборе ограничений и как NP-полная [1] задача позволяет применять её для генерации пары открытого и закрытого ключей с большой временной сложностью восстановления закрытого ключа по открытому ключу [3]. Настоящее исследование направлено на создание программной реализации данной математической модели и консольной программы на её основе.

Целью данного исследования является построение математической модели проблемы шифрования сообщения с открытым ключом, разработка вариации алгоритма