Литература

1. Кругликов, С.В. Методика решения задачи многофакторного целераспределения в автоматизированной системе управления / С.В. Кругликов // Доклады БГУИР. – 2013. – № 5. – С 93–99.

2. Липлянин, А.Ю. Методика учета важности цели при решении задачи распределения летательных аппаратов между огневыми средствами / А.Ю. Липлянин, А.С. Шеин, А.В. Хижняк // Доклады БГУИР. – 2017. – № 2. – С 77–84.

3. Городецкий, В.И.Методы и алгоритмы коллективного распознавания: обзор / В.И. Городецкий, С.В. Серебряков // Труды СПИИРАН. – 2006. – Вып. 3, т. 1. – С. 139 – 171.

АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ В АЛГОРИТМАХ ЗАЩИТЫ ИНФОРМАЦИИ

В.А. Липницкий, Л.В. Михайловская

Различные аспекты, связанные с решением алгебраических уравнений, часто и довольно неожиданно возникают при практической реализации тех или иных криптографических систем. Так, криптосистема Рабина своим базовым алгоритмом дешифрования ставит проблему решения квадратного уравнения в кольце классов вычетов по составному модулю – произведению двух простых нечетных чисел. Как ни странно, такие квадратные уравнения в общем случае имеют четыре, а не два корня.

Решение уравнения легальными пользователями сводит задачу по китайской теореме об остатках в минимальных полях Z/pZ и Z/qZ. Если p и q относятся к классу простых чисел Блюма, т.е. имеют вид $4t+3$, t – натуральное число, то задача легко решается возведением дискриминанта в строго определенную степень. Если же $p = 4t+1$, то при нечетных t существуют аналогичные формулы, а при четных t поиск квадратных корней осуществляется процедурой перебора, хотя и достаточно ограниченного перебора. Поэтому реальные пользователи криптосистемы Рабина стараются брать простые числа вида, рассмотренного в первом случае. Хакер вынужден вначале факторизовать модуль n в произведение простых множителей, т.е. решить ту же проблему, что и в криптосистеме *RSA*. Глубокое владение теорией чисел позволяет строить совершенные криптографические системы, удобные и практичные в применении.

ГРУППА АВТОМОРФИЗМОВ БЧХ-КОДА И ЕЕ ПОЛИНОМИАЛЬНЫЕ ИНВАРИАНТЫ

В.А. Липницкий, Е.В. Середа

По сути дела, группа автоморфизмов G любого БЧХ-кода порождена циклической и циклотомической подстановками, а потому является некоммутативной. Нормы синдромов – основной объект, разработанный белорусскими кодировщиками ТНС – теории норм синдромов – явились эффективными инвариантами группы Γ циклических сдвигов: норма синдрома так специфично определена через компоненты синдрома, что является одинаковой для всех векторов каждой Γ-орбиты ошибок, поэтому данный уникальный параметр и назван нормой Γ-орбиты. Выяснялось, что нормы Γ-орбит любой корректируемой совокупности векторов-ошибок попарно различны. Практическим следствием данной теории явилось семейство перестановочных норменных методов и алгоритмов коррекции ошибок БЧХ-кодами, на порядок ускоряющих работу декодеров по сравнению с традиционными синдромными алгоритмами.

В докладе рассматриваются полиномиальные инварианты всей группы G автоморфизмов БЧХ-кодов. Каждая G-орбита представляет собой объединение строго определенного ряда Γ-орбит, связанных друг с другом посредством циклотомической подстановки и ее степеней. Нормы циклотомически связанных Γ-орбит являются сопряженными элементами в конечном поле – поле определения соответствующего БЧХ-кода. Семейство взаимно сопряженных элементов поля Галуа составляет полную группу корней неприводимого полинома любого из элементов этого семейства. Согласно формулам Виета, всякий полином однозначно определяется своими корнями. Таким образом, полное семейство попарно сопряженных норм Γ-орбит, составляющих данную G-орбиту, задают однозначно определенный полином, корнями которого они являются. Это и есть полиномиальный

Библиотека БГУИР

инвариант данной *G*-орбиты. Предлагаемые полиномы являются своеобразными уникальными индикаторами каждой *G*-орбиты векторов-ошибок. Следовательно, полиномиальные инварианты могут служить основой обобщения ТНС, которая допускает укрупненную классификацию векторов-ошибок, то есть разбиение их на *G*-орбиты. Вычисление полиномиального инварианта очередной корректируемой ошибки позволит определить однозначно *G*-орбиту, которой принадлежит искомая ошибка. Дальнейший поиск ошибки будет проводится среди *Г*-орбит, входящих в данную *G*-орбиту. Данные обстоятельства резко сужают переборные элементы полиномиально-перестановочного алгоритма декодирования, что делает его более эффективным даже в сравнении с норменными методами.

ОБ АЛГОРИТМЕ ПОДСЧЕТА КОЛИЧЕСТВА ОРБИТ (0,1)-МАТРИЦ

В.А. Липницкий, Н.В. Спичекова

Матрицы как двумерные массивы информации относятся к базовым объектам высшей математики. Бинарные матрицы, то есть матрицы с элементами 0 и 1, приобрели важное значение в дискретной математике, теории графов и теории групп, теории информации и помехоустойчивом кодировании, медицине и биологии. Большой вклад в исследование класса $P(n)$ квадратных (0, 1) – матриц порядка n, содержащих в точности n единиц, внес английский математик П. Кэмерон. На исследование этого же класса матриц вышла белорусская школа помехоустойчивого кодирования [1].

Мощность класса $P(n)$ стремительно растет с ростом n. Например, $P(8)$ содержит 4 426 165 368 элементов. Поэтому целесообразно множес тво $P(n)$ делить на подклассы каким-то достаточно естественным образом. С середины XIX века в математике приобрела массовое применение идея разбиения множеств на орбиты – классы эквивалентности под действием на этих множествах тех или иных групп. Математические и технические приложения класса $P(n)$ показывают, что наиболее естественными преобразованиями матриц этого класса являются перестановки строк между собой или же перестановки столбцов между собой. Иными словами, наибольший интерес для пользователей представляют орбиты на множестве $P(n)$, которые образуются под действием квадрата симметрической группы. Естественным образом возникает задача о количестве таких орбит в классе $P(n)$.

Самый очевидный – переборный - способ вычисления количества орбит на множестве $P(n)$ представляет собой вычислительно сложную задачу. Поэтому применение класса $P(n)$ на практике предполагает разработку эффективных алгоритмов подсчета количества орбит этого множества. В докладе представлен реккурентный алгоритм подсчета количества орбит множества $P(n)$. Алгоритм основан на лемме Бёрнсайда [2]. Для нахождения числа матриц, инвариантных относительно действия фиксированной подстановки, используется линейная развертка бинарной матрицы. Получена оценка сложности предлагаемого алгоритма.

Литература

1. Цветков, В.Ю. Предсказание, распознавание и формирование образов многоракурсных изображений с подвижных объектов / В.Ю. Цветков, В.К. Конопелько, В.А. Липницкий. – Мн.: Издательский центр БГУ, 2014. – 224 с.

2. Харари, Ф. Теория графов / Ф. Харари. – М.: Мир, 1973. – 300 с.

РАСПОЗНАВАНИЕ БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ С ПОМОЩЬЮ ЦИФРОВЫХ КАМЕР МОБИЛЬНЫХ УСТРОЙСТВ

А.М. Мажейко

Отрасль биометрического определения пользователя в информационных системах с каждым годом становится все шире и шире. Если 20 лет назад биометрические считыватели использовались исключительно в специализированных целях, то в последнее десятилетие сканеры отпечатка пальца внедряются в ноутбуки и мобильные телефоны. Однако вопрос использования еще более дешевых сканеров и методов распознавания остается открытым. Одним из самых распространенных устройств ввода на мобильных устройствах являются: микрофон и фотокамера. Исследования в Томском политехническом университете показали о

Библиотека БГУИР