УДК 004.942
ББК 22.18
К 75

***Рецензенты*:**
доктор технических наук, профессор ***И. А. Калмыков***,
кандидат технических наук, профессор ***О. П. Малофей***

Кочеров Ю.Н., Червяков Н. И.

К 75 **Разработка методов и алгоритмов разделения и восстановления данных в модулярных пороговых структурах для распределенных вычислительных сетей**: монография. – Ставрополь: Изд-во СКФУ, 2016. – 239 с.

ISBN 978-5-9296-0865-0

В монографии представлены результаты комплексного исследования алгоритмов пространственного разделения информации. В работе рассмотрены и проанализированы схемы порогового разделения данных с точки зрения вычислительной сложности, выполнено их моделирование на программируемой логической интегральной схеме и проведен анализ результатов; дано описание математических моделей позволяющих модифицировать пороговые схемы, с целью повышения надежности хранения и передачи частей данных; создан комплекс программных моделей позволяющих наглядно демонстрировать результаты математических моделей.

Адресована студентам, бакалаврам, магистрам, аспирантам, научным работникам и специалистам в области информационной безопасности, занимающимся вопросами применения системы остаточных классов в криптографии.

УДК 004.942
ББК 22.18

ISBN 978-5-9296-0865-0

ŋqdqɏeɎ bɆ dədɆbɎɜə d ɞɔɑɓɔɏ Ɉqdɗɏqɏè

ВВЕДЕНИЕ

Современное общество характеризуется как информационное общество, в котором большую роль играет безопасная передача, хранение и обработка информации.

Применение пороговых схем разделения данных (СРД) в распределенных вычислительных сетях позволяет безопасно передавать части данных по проводным и беспроводным сетям и хранить их в удаленных, пространственно распределенных хранилищах. При использовании СРД только k из n абонентов пороговой схемы могут восстановить информацию. Идеи схем пороговых СРД были независимо предложены в 1979 году Ади Шамиром и Джорджем Блэкли. Важную роль при использовании СРД играет скорость разделения и восстановления информации. Использование СРД, основанных на системе остаточных классов (СОК), предложенных Миньоттом, Асмутом и Блумом, позволяют снизить время, затрачиваемое на разделение данных.

Отсутствие специализированных процессоров СРД делает актуальным разработку данных функциональных устройств. Для создания и проектирования цифровых устройств широко применяются программируемые логические интегральные схемы (ПЛИС). Это связано с тем, что логика работы ПЛИС не определяется при ее изготовлении как логика работы обычных цифровых микросхем, а создается в процессе проектирования на языках описания аппаратуры (Verilog HDH, VHDL, AHDL и др.). Применение ПЛИС для реализации СРД выдвигает дополнительные критерии их оценки, а именно, количество логических элементов (LEs) и потребляемая процессором мощность.

К недостаткам СРД относится то, что легко нарушить ее протокол или восстановить информацию по ее частям. Поэтому необходимо разработать алгоритмы, позволяющие исключить эти недостатки. Перспективным является использование многоступенчатых схем разделения данных, а также схем с применением алгоритмов кодирования.

Задача исследования состояла в разработке методов и алгоритмов схем порогового разделения данных, основанных на системе остаточных классов

ŋqdqɏeɎ bɆ dədɆbɎзə d ɕɔɑbɔɏ Ɉqddɏqɏè

Решение поставленной общей научной задачи состояло из решения следующих частных задач:

1. Анализ вычислительной сложности методов порогового разделения информации и ее восстановления.

2. Разработка моделей СРД для создания функциональных устройств специализированного процессора с целью оценки их ресурсоемкости.

3. Разработка модели и синтез схемы с разделением информации и применением алгоритма кодирования.

4. Разработка метода группового разделения данных, основанного на системе остаточных классов и его моделирование на примере обработки изображения.

5. Разработка численного метода разделения данных на основе усовершенствованной схемы Асмута-Блума с применением фрактальной геометрии.

6. Разработка комплекса программ для моделирования модулярных структур в пороговых схемах разделения информации

Для решения поставленных в работе научных задач были использованы методы теории чисел, линейной алгебры, численных методов, теории алгоритмов, комбинаторики, математического и программного моделирования, теории вероятностей, дискретной математики.

Новизна работы заключается в следующем:

1. Разработан метод, положенный в основу математической модели параллельного кодирования информации применительно к пороговым СРД, отличающийся от известных кодированием частей данных, получаемых с применением Китайской теоремы об остатках (КТО), что позволяет повысить безопасность их передачи по сетям различного исполнения.

2. Впервые разработан групповой метод порогового разделения данных, позволяющий хранить части информации в удаленных, пространственно распределенных хранилищах, отличающийся от известных применением многоступенчатой системы остаточных классов с избыточными основаниями, что обеспечивает повышенную обнаруживающую способность при восстановлении данных.

3. Предложен метод разделения данных на основе схемы Асмута-Блума с применением фрактальной геометрии. Численный

метод разделения данных на его основе позволит изменять гамму сигнала, не применяя дополнительных вычислений.

4. Разработаны модели СРД и обратного преобразования из СОК в позиционную систему счисления (ПСС), отличающиеся от известных моделей тем, что они ориентированы для реализации на ПЛИС.

5. Разработан комплекс программ и проведено компьютерное моделирование функциональных устройств специализированного процессора на языке описания аппаратуры Verilog HDL для процессора фирмы Altera.

Теоретическая значимость исследований состоит в разработке метода группового разделения данных, разработке метода порогового разделения данных с применением фрактальной геометрии, анализе вычислительной сложности преобразования из СОК в ПСС, разработке метода применения параллельных алгоритмов кодирования.

Практическая значимость исследования. Основные теоретические результаты работы доведены до уровня их практического применения в виде программного комплекса для задач моделирования модулярных структур в системах защиты информации, основанных на СОК. Разработанное программное обеспечение позволяет проводить сравнительный анализ моделей для кодирования изображений и групповой схемы разделения данных.

Реализованные методы разделения данных и точные методы преобразования из СОК в ПСС на языке описания аппаратуры Verilog HDL для процессора фирмы Altera позволяют выбирать модулярные структуры с учетом выбранных критериев.

Разработан комплекс программ моделирования параллельных алгоритмов кодирования информации, который позволяет безопасно хранить и передавать данные.

Автор выражает искреннюю благодарность научному руководителю – заслуженному деятелю науки и техники РФ, доктору технических наук, профессору, академику МАИ Червякову Н. И.

ОГЛАВЛЕНИЕ

ŋ̧qdqɏeɎ bɆ dəqɆbɎзə d ɛɑɑbɔɏ Ɉqdqɏqɏè