

ПРИМЕНЕНИЕ НЕДВОИЧНОГО МНОГОПороГОВОГО ДЕКОДЕРА ДЛЯ ЗАЩИТЫ ФАЙЛОВ ОТ ИСКАЖЕНИЙ

Овечкин П. В.

Рязанский государственный радиотехнический университет

Презентация содержит 11 слайдов

Специализированный сайт по многопороговым декодерам:
www.mtdbest.iki.rssi.ru

Процесс передачи информации



помехи



запись



чтение



помехи (царапины, отпечатки пальцев)



Специализированный сайт по многопороговым декодерам:

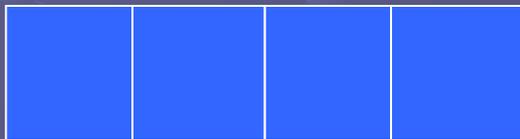
www.mtdbest.iki.rssi.ru

Помехоустойчивое кодирование

Одним из важнейших методов снижения вероятности ошибки при передаче данных по каналам с шумами является использование методов помехоустойчивого кодирования

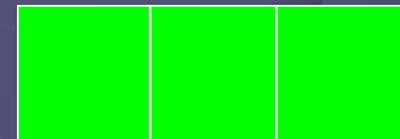
Кодирование - это введение избыточности в передаваемое сообщение

k - информационные символы



+

r - избыточные символы



Специализированный сайт по многопороговым декодерам:

www.mtdbest.iki.rssi.ru

Помехоустойчивое кодирование для защиты информации в системах хранения

В магнитных и оптических запоминающих устройствах применяются недвоичные коды

Коды Рида-Соломона – наиболее популярные недвоичные коды

- Декодер эффективно исправляет пакеты ошибок
- Вычислительная сложность декодирования $O(n^2)$

Специализированный сайт по многопороговым декодерам:

www.mtdbest.iki.rssi.ru

Программы для защиты информации на магнитных и оптических носителях

Для дополнительной защиты данных на магнитных и оптических носителях используются коды Рида-Соломона и кодирование/декодирование на базе матриц Вандермонда

Наиболее известные программы для дополнительной защиты файлов:

- QuickPar;
- ICE ECC.

Вычислительная сложность декодирования $O(n^3)$

Специализированный сайт по многопороговым декодерам:

www.mtdbest.iki.rssi.ru

Недвоичные многопороговые декодеры

Недвоичный многопороговый декодер – простейший декодер мажоритарного типа

Основные преимущества недвоичных многопороговых декодеров

- Простота практической реализации (низкая стоимость, высокая надежность, высокое быстродействие);
- Эффективный алгоритм исправления ошибок;
- Сложность декодирования $O(n)$;
- Не используются вычисления в полях Галуа.

Специализированный сайт по многопороговым декодерам:

www.mtdbest.iki.rssi.ru

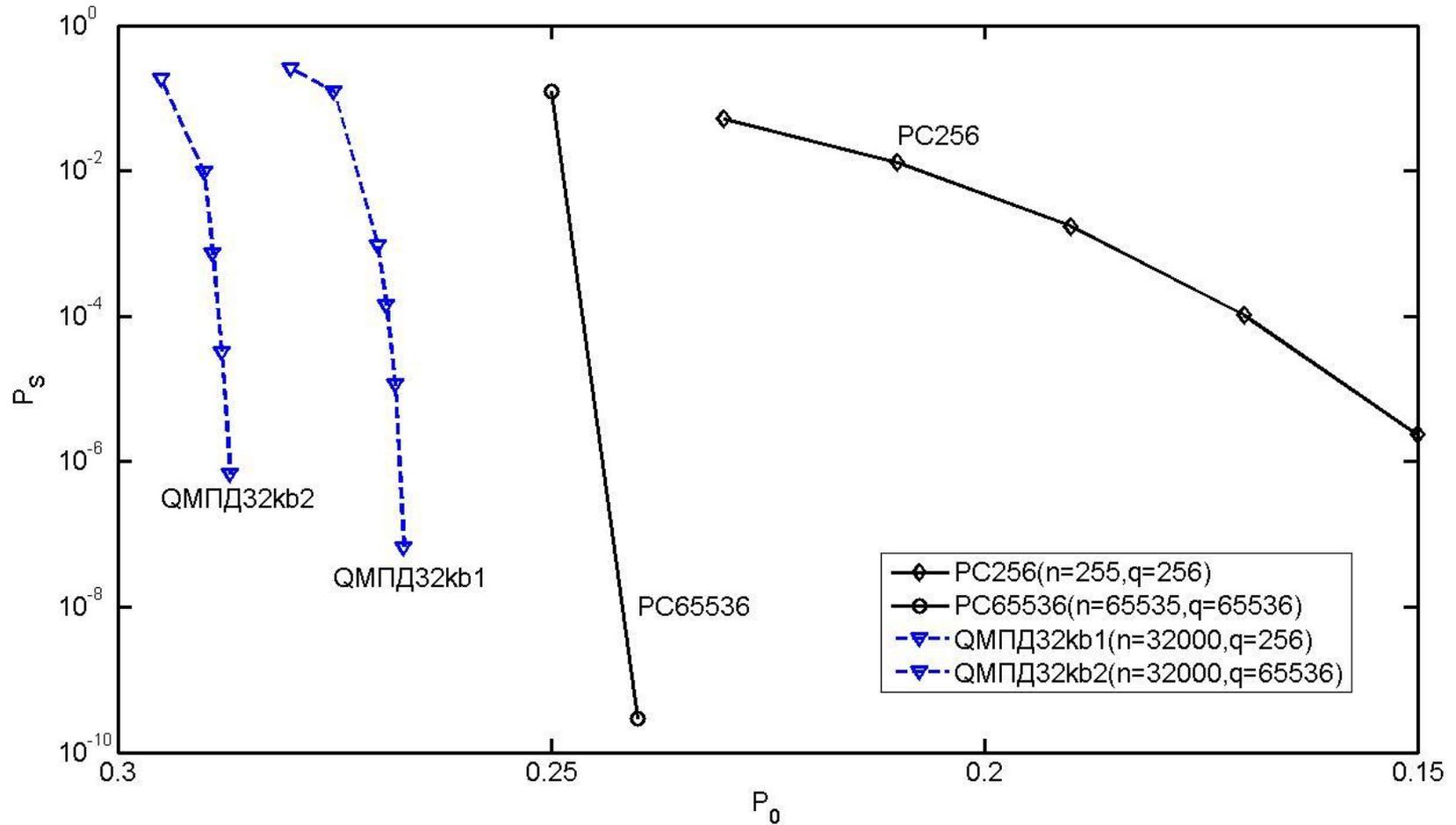
Схема недвоичного многопорогового декодера



Специализированный сайт по многопороговым декодерам:

www.mtdbest.iki.rssi.ru

Эффективность недвоичного МПД для $R=1/2$



Специализированный сайт по многопороговым декодерам:

www.mtdbest.iki.rssi.ru

Использование QMPD для защиты файлов от искажений

The image displays the MTDprotect software interface, which is used for file protection and decoding. The central window, titled "Картина проверки файла" (File Check Picture), shows a green grid representing the file's data. The file being checked is "F:\bd.rar", and the check file is "F:\bd.rar.nse". The block size is set to 8, and the page number is 1. The interface is divided into three main sections:

- Left Panel (Decoding):** Shows the process of decoding a corrupted file. The input file is "F:\bd.rar" and the check file is "F:\bd.rar.qmtd". The restored file is "F:\bd.rar.rep". The "МПД" (QMPD) option is selected. The "Декодировать" (Decode) button is visible.
- Right Panel (Encoding):** Shows the process of encoding a file. The file to be encoded is "F:\bd.rar" and the check file is "F:\bd.rar.qmtd". The original file size is 703.70 Мбайт. The protection quality is set to "Отличная защита - 100%". The check file size is also 703.70 Мбайт. The "Создать" (Create) button is visible.
- Bottom Panel (Status):** Shows the progress and completion status of the operations. The left status bar indicates that decoding is completed successfully, with a speed of 3.71 Мбайт/с and a clean speed of 132.90 Мбайт/с. The right status bar indicates that encoding is completed, with a speed of 4.22 Мбайт/с and a clean speed of 37.16 Мбайт/с.

Специализированный сайт по многопороговым декодерам:

www.mtdbest.iki.rssi.ru

Сравнение программ для защиты файлов

	ICE ECC	QuickPar	MTDProtect
Время кодирования	1 час	1.5 часа	1 минута
Время восстановления файла с однобитовой ошибкой	3 минуты	3 минуты	1 минута
Время восстановления файла, с поврежденным блоком размером 50% от размера файла	1 час	1 час	1.5 минуты
Время восстановления файла с независимыми ошибками, $P_0=0.1$	невозможно	невозможно	7 минут

Основные преимущества использования QМПД для защиты файлов от искажений:

- скорость кодирования/восстановления выше в десятки, а иногда и в сотни раз по сравнению с известными программами-аналогами;
- Эффективное исправление как пакетов ошибок, так и независимых ошибок

Специализированный сайт по многопороговым декодерам:

Большой объем научных и учебных материалов по
многопороговым декодерам можно найти на
специализированном сайте ИКИ РАН:
www.mtdbest.iki.rssi.ru

Спасибо за внимание