Возможности и особенности

способа передачи и

комплексной защиты информации

Функциональные особенности способа

- *универсальность* – возможность применения в любых хранилищах информации и каналах связи (с разной интенсивностью помех и законом их распределения);
- *комплексность защиты* - возможность защитить информацию при различных видах воздействия на нее в рамках одного алгоритма обработки информации и при однократном введении избыточности.

Количественные особенности способа

- *высокая скорость* обработки информации;
- *гарантированная достоверность* в произвольном канале;
- *высокая кратность* исправляемых ошибок.

Способ передачи и комплексной защиты информации основан на применении новых кодов для восстановления целостности информации – стохастических кодов.

Процедура стохастического кодирования

Кодирование сводится к применению любых двоичных (n,k)-кодов с исправлением ошибок, описываемых проверочной матрицей H и кодовым расстоянием d, в виде l-перемежения блоков кода.

При этом l одноименных (первых, вторых, …, l) двоичных символов рассматривается как q-ичный символ ($q=2^l$).

Каждый q-ичный символ до передачи в канал подвергается рандомизации (стохастическому преобразованию) со сменой параметра рандомизации для каждого нового символа.

Операция рандомизации выполняется по правилам криптографии Шеннона.

Процедура декодирования

- обратная рандомизация q-ичных символов;
- предварительное выделение (локализация) неискаженных в канале q-ичных символов;
- проверка точности выделенных символов по принципу солидарного (согласованного) декодирования отдельных двоичных l перемежений кодового блока;
- исправление ошибочных символов через достоверно выделенные символы.

Основное отличие стохастических кодов от классических кодов с исправлением ошибок

Классические коды исправляют ошибки по принципу максимума правдоподобия.

Применение этого принципа приводит на практике к невозможности использования классических кодов с исправлением ошибок в реальных каналах связи.

Стохастические коды исправляют ошибки по принципу максимума точности, который позволяет обеспечить требуемую наперед заданную достоверность информации после декодирования.

Обобщенная эффективность стохастических методов защиты

Можно говорить о «максимуме пользы» (максимальной вероятности доведения сообщения, минимальной вероятности ошибки декодирования, минимальной вероятности навязывания ложной информации, минимальной вероятности вскрытия содержания конфиденциального сообщения) при минимальных вложениях (введении минимальной избыточности, требуемой сложности обработки, минимальном времени задержки)

Скорости обработки для декодирования и отдельных операций, полученные на модели (для процессора с тактовой частотой 1467МГц)

Скорость декодирования достигает 50 Мбит/сек и практически не зависит от параметров кода и от вероятности возникновения ошибок.

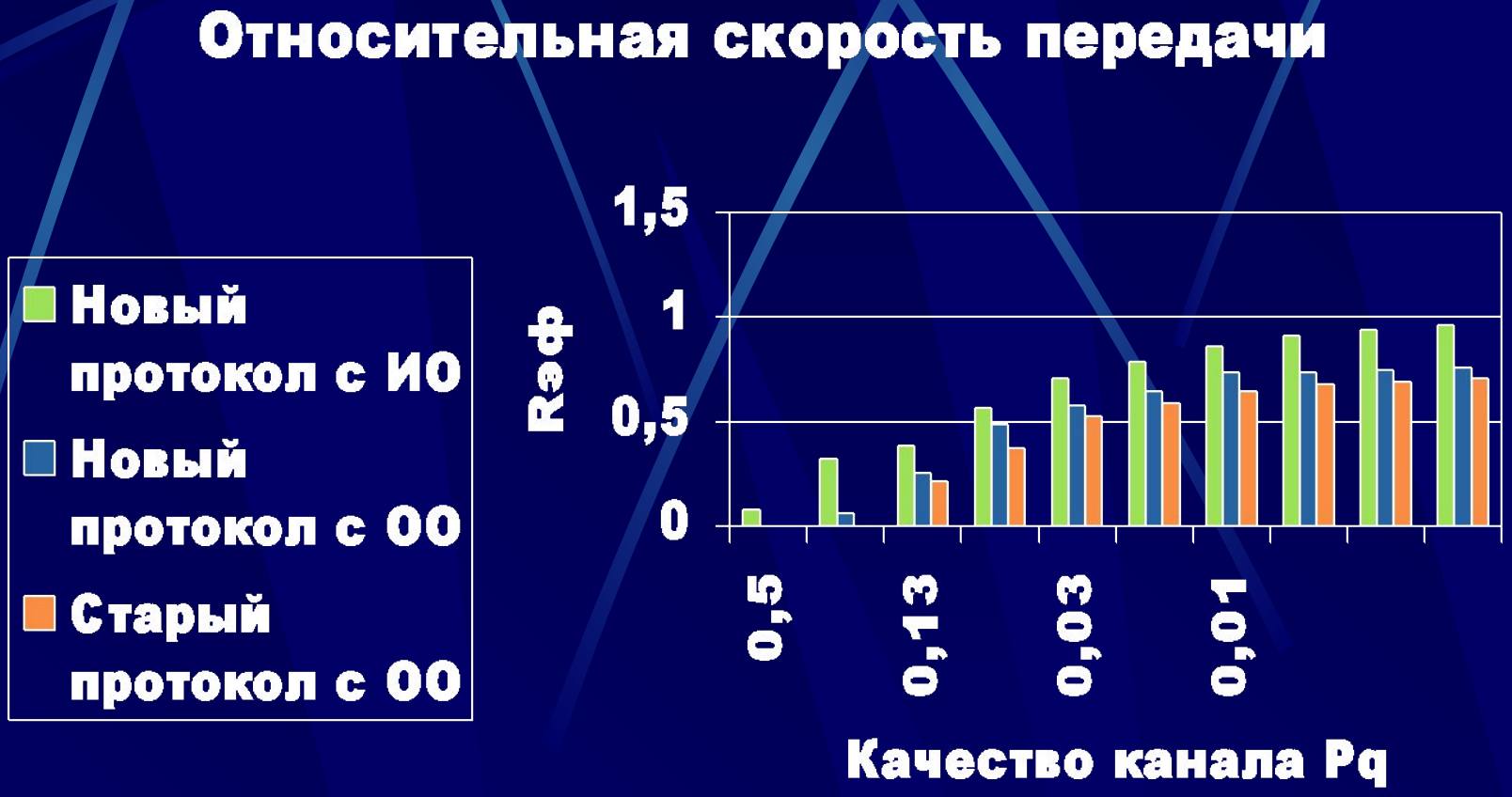
Скорость прямого стохастического преобразования 77 097 312 бит/сек.

Скорость обратного стохастического преобразования 65 154 628 бит/сек.

Скорость передачи при выборе оптимальных значений кода с исправлением ошибок

Pq код	2^{-1}	2^{-2}	2^{-3}	2^{-4}	2^{-5}	2^{-6}	2^{-7}	2^{-8}	2^{-9}	2^{-10}
(8,2)	0.079	0.149								
(8,4)		0.212	0.364							
(16,7)		0.320	0.388							
(16,11)			0.339	0.572	0.632					
(32,26)				0.424	0.705	0.774				
(64,57)					0.481	0.788	0.866			
(128,120)							0.836	0.917		
(256,247)								0.864	0.945	
(512,502)									0.890	0.962

Сравнение методов передачи



Выигрыш в скорости передачи по каналам связи

- при качестве двоичного канала, оцениваемой вероятностью искажения двоичного символа от 10^{-1} до 10^{-2} (другие методы вообще не работают) достигается относительная (эффективная) скорость 0,1 – 0,3;
- при качестве канала от 10^{-2} до 10^{-3} – по сравнению с применяемыми каскадными кодами с исправлением ошибок достигается выигрыш в 1,5-2 раза (от 0,3-0,5 до 0,75);
- при качестве канала от 10^{-3} до 10^{-5} – по сравнению с циклическими кодами достигается выигрыш в 1,5-1,7 раза (от 0,6-0,7 до 0,95).

Выигрыш в методах контроля и восстановления целостности

- при попытках навязывания ложной информации обеспечивается контроль и восстановление целостности в режиме имитостойкого исправления ошибок.

Выигрыш в решении задач криптографии

- высокая скорость обработки (10 мбайт/с);
- большой размер ключа (2 кбайт);
- стойкость, близкая к абсолютной по Шеннону.

Сферы применения стохастических методов защиты информации

- протоколы передачи информации по любым каналам связи;
- протоколы защиты информации, где используются методы криптографической защиты от ознакомления и навязывания ложной информации;
- методы и протоколы контроля и восстановления целостности информации в компьютерных системах.

Правовой статус

- Способ передачи и комплексной защиты информации признан в Российской Федерации изобретением. На него выдан патент №2367007, удостоверяющий правовую охрану способа с 30 августа 2007 года.
- На основании международной заявки PCT/RU2007/000580 в настоящее время оформляется получение патентов в Европе (Европатент), в США, в Японии, Китае и Индии.