

Слайд 1

Уважаемый Председатель и уважаемые члены ГЭК. Вашему вниманию предлагается дипломная работа на тему – Устройства закрытия речевых сигналов.

Слайд 2

Методы против подслушивания, прежде всего, направлены на предотвращение утечки информации с простых гидроакустических и сейсмических каналов. Для повышения скорости перехвата используются сложные каналы утечки информации, в том числе электронные с использованием интегрированных устройств, РЧ и оптической системы. При этом защита информации от передачи содержит методики и средства для блокировки любых каналов, в которых происходит утечка звукового или аудио данного. Защита разговоров с телефоном осуществляется активными и пассивными методами. Передача речевых данных является фундаментом коммуникаций в обществе человека, защита ее является основным вопросом защиты. Речевая информация передается через канал связи, при увеличении длины ключей увеличивается время его выявления. Чтобы структурно сократить речевые данные в связи, используется шифрование и техническое блокирование. В криптографии аналоговые речевые сигналы с микрофона приводятся в реорганизацию с помощью аналогового цифрового преобразователя к цифровому сигналу. При аналогичном и цифровом преобразовании, амплитуды сигнала измеряются одинаковым интервалом времени, называемым фазой дискреции. Закрытие звукового сигнала узкополосного телефона осуществляется техническим или аналоговым методом маски. Эти методы получили название скремблеры перемешиваний. Скремблинг отличается от криптографической скрембляция тем, что в шифровании сообщение скрыто в символе, а в техническом зашифровании скрыто речевой сигнал, не превращаясь в цифру. При технических замыканиях характеристики начальных речевых сигналов модифицируются так, что они делаются аналогичным шуму, но занимают одну и ту же частотную полосу. Это дает возможность передавать скремблированные сигналы в обычных типовых телефонных каналах.

Слайд 3

Подавители могут быть реализованы как программное или аппаратное устройство, которое обрабатывает аналоговые или цифровые голосовые сигналы в течение времени. В результате сигналы теряют свою семантическую ценность и становятся неразличимыми для посторонних лиц, либо на выходе скремблера появляется случайная битовая последовательность. Побитовое цифровое скремблирование получается несложным наложением битов речевого сигнала на биты гаммы, см. рис. Важнейшим моментом в схеме является синхронизация гаммовых генераторов на стороне приема и переноса инфекций. Этот ход решается путем передачи в последовательности информации параметров

генератора, либо путем специальных синхронических кадров или отдельного канала соединения.

Слайд 4

Качество восстановления сигналов зависит от самого метода установки помех, а также от других параметров. Рис. Помехи в радиосвязи могут возникать от пересеченной местности или движения приемника либо передатчика.

Слайд 5

Метод временного преобразования сигнала – отрезок речи определенной длительности делится на части – фрагментов или отрезков и затем смешивается по определенному правилу. Качество шифрования повышается по мере уменьшения длительности перетасовываемых сегментов. Обратите внимание, что по мере увеличения продолжительности сегмента сигнала, зашифрованного в аппаратном или программном устройстве, увеличивается задержка перед передачей речи. Визуальное представление операции обращения сигнала во времени показано на рисунке. Здесь сегмент сигнала (слева), начиная с момента времени 0, инвертируется для получения нового сигнала (справа).

Слайд 6

Ход временной перестановки показан на рисунке. Сегмент сигнала делится на 4 фрагмента, в непринужденных порядках 1-2-3-4 и потом эти фрагменты переходят в измененный порядок 2-4-1- 3.

Слайд 7

Скремблирование в области частоты осуществляется на спектре частоты, а именно на самом спектре сигнала, который выражается в виде функции зависимости времени. На рис. представлен частотный спектр русских звуков. Человеческая речь имеет обширную полосу частот приблизительно 50 – 10 000 Гц, человеческое ухо способно распознать звуки в диапазоне 20 Гц – 25 000 дБ. В вокальном спектре выделяют частоты, в которых сконцентрирована ключевая деятельность сигнала и эти частоты именуют формантами. В русской речи распознают 5 формантов, но для ее удовлетворительного распознавания слушателем полно присутствие в сигнале лишь первых двух-трех формант. Это облегчает передачу речи по беспроводным или проводным сетям связи.

Слайд 8

Сочетая временной и частотной скремблер, можно значительно улучшить закрытие речи. Комбинированный скремблер значительно сложнее обыкновенных, и приводят к компромиссу при выборе уровня закрытия и остаточной разборчивой сигнала. Часть разных систем, которые работают на этом принципе, была урезано измышлениями разработчика. В качестве примера такой

системы мы посмотрим скремблер, схему которого можно увидеть на рис. В данном скремблере операции частотной и временной перестановки дискретного сегмента речевой сигнала осуществляются через четыре процессора цифрового сигнала, одна из которых может выполнять функцию ПСП-генератора. Степень закрытия речи, может значительно повысить с помощью сочетания быстро-частотной шифровки. Комбинированные скремблеры не столь сложны, как обычные скремблеры, и вызывают компромиссы в плане уровня запуска, периода задержки, остатков разборчивости и количества искажений в ранее созданных сигналах, сложности систем.

Слайд 9

Биты переноса C1, C2 и C3 сумматоров OR1, OR2 и OR3 используются, как управляющие биты. В зависимости от состояния их, синхронизация решает, которые регистры необходимо сдвигать. Если все C1, C2 и C3 одинаковые, то изменение происходит в каждом из трех регистров. И если два переносных бита имеют одно и то же состояние, они сдвигаются в соответствующих регистрах. Изменение происходит на 8 циклах. Сейчас неизвестно, как взламывать этот шифр, что позволяет использовать этот шифр, что позволяет защитить криптографическую информацию.

Слайд 10

На рис показано представление РСЛОС, соответствующее этому полиному. В процессе работы значения операции генератора, содержащиеся в ячейках, сдвигаются вправо и самый левый бит в регистре заменяется битом, полученным применением операции «только или» последовательно к битам, содержащимся в ячейках с номерами 7, 5 и 2. Для создания качественного РСЛОС, способного генерировать последовательность чисел с требуемым периодом и устойчивого к взлому, необходимо знать упомянутые выше свойства порождающих полиномов. В настоящее время эти свойства хорошо изучены математиками, что делает РСЛОС чрезвычайно перспективным инструментом в криптографии.

Слайд 11

Тесты, которые выдают результаты графически, требуют от человека интерпретации. Таким образом, не может быть использовано для автоматического процесса проверок псевдослучайных цепочек и прочих «причинных» цепочек. Пример результата графического тестирования показан на рисунке. Здесь по абсциссовой оси абсцисс отражены все сочетания из 3-х битов, а по ординате — разница частоты возникновения этого сочетания в последовательности $1/N$, где N - общее число комбинаций, т.е. в этом случае 8. Численный статистический тест может автоматически сравнивать полученные результаты с определенным уровнем и на основании этого решать, успешно ли он прошел тот или иной тест. Чтобы получить более точную оценку, можно несколько раз провести тесты и рассчитывать вероятность того или иного результата в результате. В ряде случаев

для того, чтобы получить точность теста, необходимо увеличить число псевдослучайного значения, поступающего на вход теста.

Слайд 12

Программное обеспечение выполнено в виде графических приложений для компьютеров, работающих под операционной системой, поддерживаемой исполняемой средой Qt5 Windows, Linux и MacOS. На рис. показано окно главного окна программы. В ходе обзора программных алгоритмов генерации псевдослучайных последовательностей чисел и псевдослучайных перестановок, р были рассмотрены алгоритмы такие, как средней квадратной метод сравнения, линейно-полиномиальные методы сравнения, аддитивных генераторов, генераторов на основе линейно-нелинейных регистров, генераторов на основе линейно-нелинейных обратных связей, комбинаций генераторов постоянного и переменного времени. В числе алгоритмов псевдослучайной генерации рассматриваются тривиальные алгоритмы, алгоритм Дональда Кнута, алгоритм Фишера-Йейта. Также были проанализированы методики проверки статистической псевдослучайной битовой строки на близость к настоящей вероятности. Рассмотрены разные тестовые наборы и выбраны несколько тестовых наборов из набора NIST для выполнения программного скремблера. Разработана программа для оцифровки речевых сигналов с помощью языка C++ и библиотеки Qt5. Реализованы такие подсистемы, как: подсистема вывода и вывода сигналов, подсистема генерирования псевдослучайного числа и перестановки и так далее. Результаты выпускной квалифицированной работы можно использовать для того, чтобы защитить конфиденциальность речи при помощи разработанной программы и анализировать работу скриптов с различными характеристиками.

Слайд 13

Таким образом, Цель работы достигнута. Спасибо за внимание!