ЗИСОПД

Лекция
Скремблирование и дескремблирование

Скремблер (scramble — шифровать, перемешивать) — программное или аппаратное устройство (алгоритм), выполняющее скремблирование — обратимое преобразование цифрового потока без изменения скорости передачи с целью получения свойств случайной последовательности. После скремблирования появление «1» и «0» в выходной последовательности равновероятны. Скремблирование — обратимый процесс, то есть исходное сообщение можно восстановить, применив обратный алгоритм.

Применительно к телекоммуникационным системам скремблирование повышает надежность синхронизации устройств, подключенных к линии связи (обеспечивает надежное выделение тактовой частоты непосредственно из принимаемого сигнала), и уменьшает уровень помех, излучаемых на соседние линии многожильного кабеля. Другая область применения скремблеров — защита передаваемой информации от несанкционированного доступа.

Для алгоритмов скремблирования исключительно важны скорость работы и случайный характер последовательности, чтобы его нельзя было восстановить в случае несанкционированного перехвата. Процесс скремблирования может включать в себя добавление определенных компонент к исходному сигналу либо изменение важных частей сигнала для того, чтобы усложнить восстановление вида исходного сигнала либо для придания сигналу определенных свойств.

Скремблеры применяются в телефонных сетях общего пользования, спутниковой и радиорелейной связи, цифровом телевидении, а также для защиты лазерных дисков от копирования. Обычно скремблирование осуществляется на последнем этапе цифровой обработки непосредственно перед модуляцией.

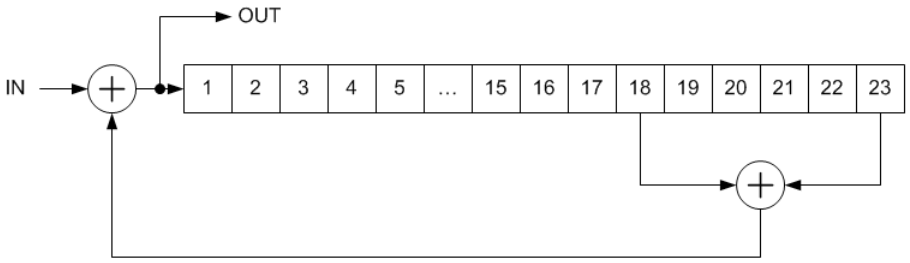
Принцип скремблирования заключается в побитном изменении проходящего через систему потока данных. Основной операцией, используемой в скремблерах, является побитовый XOR.

Типы скремблеров:

- Самосинхронизирующиеся скремблеры
- Аддитивные скремблеры (с установкой)

<u>Самосинхронизирующиеся скремблеры</u>

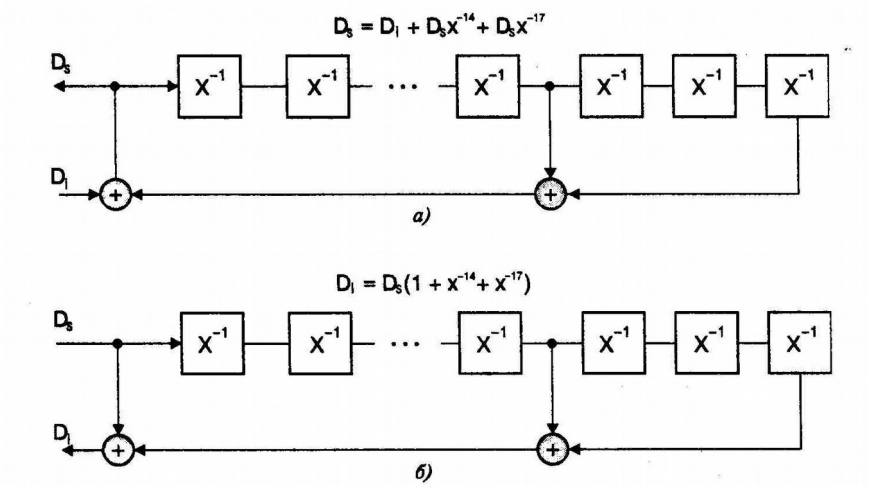
Основной частью самосинхронизирующегося скремблера является генератор псевдослучайной последовательности (ПСП) в виде линейного n-каскадного регистра с обратными связями, как правило формирующий последовательность максимальной длины $2^n - 1$.



Особенностью самосинхронизирующегося скремблера является то, что он управляется скремблируемой последовательностью, то есть той, которая передаётся в канал. Поэтому при данном виде скремблирования не требуется специальной установки состояний скремблера и дескремблера: скремблированная последовательность записывается в регистры сдвига скремблера и дескремблера, устанавливая их в идентичное состояние. При потере синхронизма между скремблером и дескремблером время восстановления синхронизма не превышает числа тактов, равного числу ячеек регистра скремблера.

На приёмной стороне выделение исходной последовательности происходит путём сложения по модулю 2 принятой скремблированной последовательности с последовательностью на выходе сдвигового регистра. Например, для схемы, приведенной на рисунке, входная последовательность IN с помощью скремблера в соответствии с соотношением $OUT = IN \oplus (R_{18} \oplus R_{23})$ преобразуется в посылаемую двоичную последовательность OUT. В приёмнике из этой последовательности таким же регистром сдвига, как на приёме, формируется последовательность $IN` = OUT \oplus (R_{18} \oplus R_{23}) = IN \oplus (R_{18} \oplus R_{23}) \oplus (R_{18} \oplus R_{23}) = IN$.

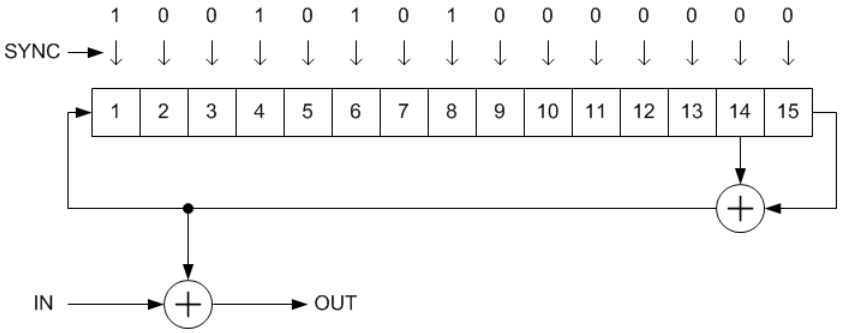
Как следует из принципа действия схемы, при одной ошибке в последовательности IN ошибочными получаются также последующие восемнадцатый и двадцать третий символы (в данном примере). В общем случае влияние ошибочно принятого бита будет сказываться *a* раз, где *a* — число обратных связей в регистре сдвига. Таким образом, самосинхронизирующийся скремблер-дескремблер обладает свойством размножения ошибок. Данный недостаток самосинхронизирующегося скремблера-дескремблера ограничивает число обратных связей в регистре сдвига; практически это число не превышает $a = 2$.
Для примера приведены скремблер и дескремблер, используемые в протоколе V.22.



Второй недостаток самосинхронизирующегося скремблера связан с возможностью появления на его выходе при определенных условиях так называемых «критических ситуаций», когда выходная последовательность приобретает периодический характер с периодом, меньшим длины ПСП. Чтобы предотвратить это, в скремблере и дескремблере предусматриваются специальные дополнительные схемы контроля, которые выявляют наличие периодичности элементов на входе и нарушают её.

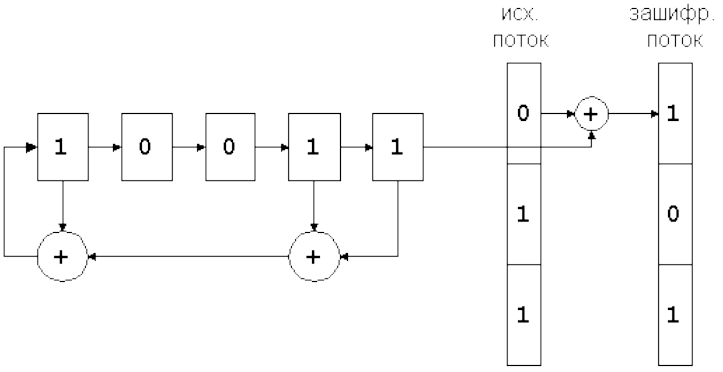
Аддитивные скремблеры

При аддитивном скремблировании требуется предварительная идентичная установка состояний регистров скремблера и дескремблера. В скремблере с установкой, как и в самосинхронизирующемся скремблере, производится суммирование входного сигнала и ПСП, но результирующий сигнал не поступает на вход регистра. В дескремблере скремблированный сигнал также не проходит через регистр сдвига, поэтому размножения ошибок не происходит.



Суммируемые в скремблере последовательности независимы, поэтому их период всегда равен наименьшему общему кратному величин периодов входной последовательности и ПСП и критическое состояние отсутствует. Отсутствие эффекта размножения ошибок и необходимости в специальной логике защиты от нежелательных ситуаций делают способ аддитивного скремблирования предпочтительнее.

Рассмотрим другой вариант аддитивного скремблера (x^5+x^4+x+1).



Изображенный на рисунке скремблер записывается комбинацией "10011_2" — единицы соответствуют разрядам, с которых снимаются биты для формирования обратной связи.

Пример кодирования информационной последовательности 010111_2 скремблером 101_2 с начальным ключом 110_2.

```
скремблер  код.бит   инф.бит   рез-т
 1 1 0  _
  \ \    \_
 1 1 1   _  \_
  \ \    \_   0   XOR   0    =   0
 0 1 1   _  \_
  \ \    \_   1   XOR   1    =   0
 1 0 1     \_
  \ \        1   XOR   0    =   1
и т.д.
```

Реализация скремблера возможна как на электронной, так и на электрической базе, что и обеспечило его широкое применение. Факт, что каждый бит выходной последовательности зависит только от одного входного бита, также упрочил положение аддитивных скремблеров в защите данных. Это связано с неизбежно возникающими в канале передаче помехами, которые могут исказить в этом случае только те биты, на которые они приходятся.

Декодирование заскремблированных последовательностей происходит по той же самой схеме, что и кодирование.

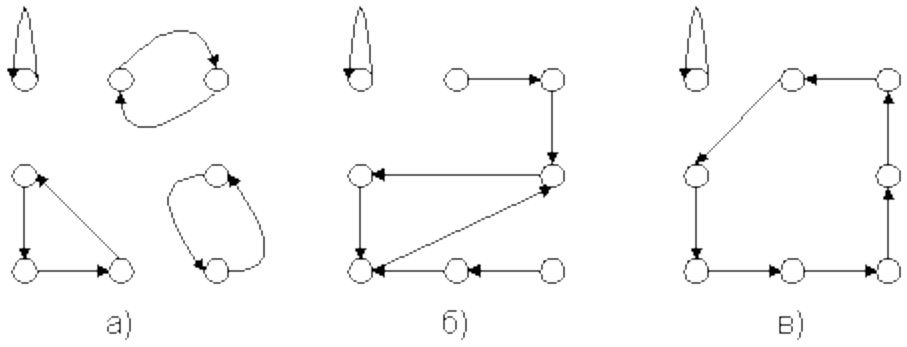
Главная проблема аддитивных скремблеров — синхронизация передающего (кодирующего) и принимающего (декодирующего) устройств. При пропуске или ошибочном вставлении хотя бы одного бита вся передаваемая информация необратимо теряется. Поэтому, в системах на основе аддитивныъх скремблеров очень большое внимание уделяется методам синхронизации. На практике для этих целей обычно применяется комбинация двух методов: а) добавление в поток информации синхронизирующих битов, заранее известных приемной стороне, что позволяет ей при ненахождении такого бита активно начать поиск синхронизации с отправителем, и б) использование высокоточных генераторов временных импульсов, что позволяет в моменты потери синхронизации производить декодирование принимаемых битов информации "по памяти" без синхронизации.

Число бит, охваченных обратной связью, то есть разрядность устройства памяти для порождающих кодирующую последовательность бит называется разрядностью скремблера. Изображенный выше скремблер имеет разрядность 5. Чем больше разрядность скремблера, тем выше криптостойкость системы, основанной на его использовании.

При достаточно долгой работе скремблера неизбежно возникает его зацикливание. По выполнении определенного числа тактов в ячейках скремблера создастся комбинация бит, которая в нем уже однажды оказывалась, и с этого момента кодирующая последовательность начнет циклически повторяться с фиксированным периодом. Данная проблема неустранима по своей природе, так как в N разрядах скремблера не может пребывать более 2^N комбинаций бит, и, следовательно, максимум, через, 2^N-1 циклов повтор комбинации обязательно произойдет. Комбинация "все нули" сразу же

исключается из цепочки графа состояний скремблера — она приводит скремблер к такому же положению "все нули". Это указывает еще и на то, что ключ "все нули" неприменим для скремблера. Каждый генерируемый при сдвиге бит зависит только от нескольких бит хранимой в данный момент скремблером комбинации. Поэтому после повторения некоторой ситуации, однажды уже встречавшейся в скремблере, все следующие за ней будут в точности повторять цепочку, уже прошедшую ранее в скремблере.

Возможны различные типы графов состояния скремблера. На рисунке ниже приведены примерные варианты для 3-разрядного скремблера. В случае "А" кроме всегда присутствующего цикла "000"→"000" есть ещё три цикла – два с двумя состояниями и один с тремя. В случае "Б" мы видим цепочку, которая сходится к циклу из 3 состояний и уже никогда оттуда не выходит. И наконец, в случае "В" все возможные состояния кроме нулевого, объединены в один замкнутый цикл. Очевидно, что именно в этом случае, когда все 2^N-1 состояний системы образуют цикл, период повторения выходных комбинаций максимален, а корреляция между длиной цикла и начальным состоянием скремблера (ключом), которая привела бы к появлению более слабых ключей, отсутствует.



Для скремблера любой разрядности N всегда существует такой выбор охватываемых обратной связью разрядов, что генерируемая ими последовательность бит будет иметь период, равный 2^N-1 битам. Так, например, в 8-битном скремблере, при охвате 0-го, 1-го, 6-го и 7-го разрядов за время генерации 255 бит последовательно проходят все числа от 1 до 255, не повторяясь ни разу.

Схемы с выбранными по данному закону обратными связями называются генераторами последовательностей наибольшей (максимальной) длины (ПНД, ПМД), и именно они используются в скремблирующей аппаратуре. Из множества генераторов ПНД заданной разрядности во времена, когда они реализовывались на электрической или минимальной электронной базе выбирались те, у которых число разрядов, участвующих в создании очередного бита, было минимальным. Обычно генератора ПНД удавалось достичь за 3 или 4 связи. Сама же разрядность скремблеров превышала 30 бит, что давало возможность передавать более 2^{30} бит > 100 Мбайт информации без опасения начала повторения кодирующей последовательности.

Достаточно чтобы полином степени N не был представим по модулю 2 в виде произведения никаких других полиномов, для того, чтобы скремблер, построенный на

его основе, создавал ПНД. Например, неприводимым полиномом степени 3 является x^3+x+1, в двоичном виде он записывается как 1011_2 (единицы соответствуют присутствующим разрядам). Скремблеры на основе неприводимых полиномов образуются отбрасыванием самого старшего разряда (он всегда присутствует, а следовательно, несет информацию только о степени полинома), так на основе указанного полинома, мы можем создать скремблер 011_2 с периодом зацикливания $7=2^3-1$. Естественно, что на практике применяются полиномы значительно более высоких порядков.

Скремблирование для защиты телефонных переговоров и радиосвязи

Скремблеры активно применяются для защиты телефонных и радио переговоров. При скремблировании возможно преобразование речевого сигнала по трем параметрам: амплитуде, частоте и времени. В системах подвижной радиосвязи практическое применение нашли в основном частотные и временные преобразования сигнала, а также их комбинации. Возможные помехи в радиоканале существенно затрудняют точное восстановление амплитуды речевого сигнала, в связи с чем амплитудные преобразования при скремблировании практически не применяются.

Основные характеристики

Основные технические характеристики аналоговых скремблеров:

- уровень закрытия информации,
- остаточная разборчивость,
- качество восстановления сигнала.

Если для цифровых СПД понятие уровня закрытия строго регламентируется и определяется криптографической стойкостью информации, то для аналоговых скремблеров (особенно в системах подвижной радиосвязи) данное понятие носит условный характер, так как к настоящему времени на этот счет не выработано четких стандартов или правил. В ряде случаев в качестве критериев уровня закрытия информации при сравнении различных средств подвижной радиосвязи с аналоговым скремблированием можно использовать количество ключевых параметров и количество возможных ключей скремблера.
Под *ключевым параметром аналогового скремблера* обычно понимают *какой-либо параметр преобразования речевого сигнала, значение которого необходимо знать для осуществления обратного преобразования сигнала на приемной стороне*.

Ключом аналогового скремблера называют *конкретное секретное состояние некоторых параметров преобразования речевого сигнала*. Количество ключей скремблера определяется множеством всевозможных значений ключа. Для скремблеров с одним ключевым параметром оно определяется числом возможных состояний этого параметра, для скремблеров с несколькими ключевыми параметрами — количеством возможных комбинаций значений этих параметров (как правило, произведением чисел состояний всех ключевых параметров).

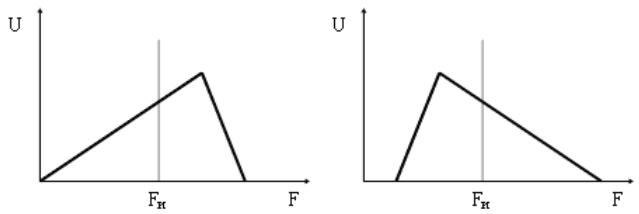
Качество восстановления сигнала определяется искажениями сигнала при его частотных или временных преобразованиях. Эта характеристика отражает разборчивость и узнаваемость восстановленной речи. Приемлемым или коммерческим качеством восстановленной на приемном конце речи считается такое, когда слушатель без усилий может определить голос говорящего и смысл произносимого сообщения. Наилучшим качеством восстановления сигнала обладают частотные инверторы, которые практически не ухудшают разборчивость и узнаваемость речи при правильной реализации. Более сложные методы частотных преобразований могут вносить некоторые искажения в речевой сигнал. Реализация высокого качества восстановления речи при временных преобразованиях требует достаточно сложной обработки.

Под *остаточной разборчивостью* понимают *процент восстановленных фрагментов скремблированного речевого сигнала при прослушивании переговоров с помощью обычных УКВ-приемников или радиостанций, не оснащенных аналогичным скремблером*. Подавляющее большинство известных аналоговых речевых скремблеров в той или иной мере сохраняют остаточную разборчивость. В прослушиваемом речевом сигнале, защищенном скремблером, сохраняется информация о темпе речи, улавливаются паузы. При несложных способах защиты опытный оператор может разобрать (в зависимости от наличия сведений о тематике ведущихся переговоров) от 10 до 50% передаваемой информации.

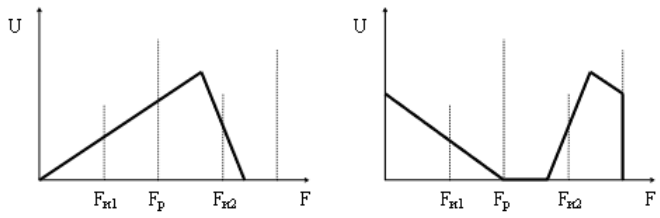
Основные методы преобразования речевого сигнала:

- Частотные преобразования
  - Частотная инверсия сигнала
  - Разбиение полосы частот речевого сигнала на несколько поддиапазонов и частотная инверсия спектра сигнала в каждом поддиапазоне относительно средней частоты поддиапазона
  - Разбиение полосы частоты речевого сигнала на несколько поддиапазонов и их частотные перестановки
- Временные преобразования
  - Инверсия по времени сегментов речи
  - Временные перестановки сегментов речевого сигнала
- Комбинированные методы

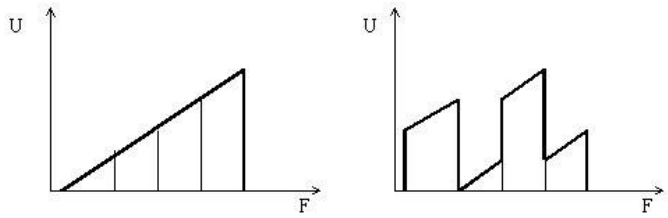
Частотные преобразования



При *частотной инверсии* преобразование спектра речевого сигнала эквивалентно повороту частотной полосы сигнала вокруг некоторой средней частоты $F_и$ — частоты инверсии.



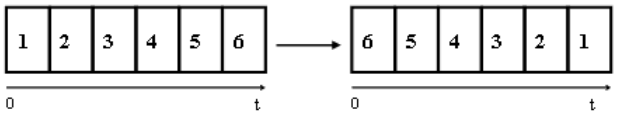
Скремблер с разбиением полосы речевого сигнала на поддиапазоны с частотной инверсией сигнала в каждом поддиапазоне (*полосно-сдвиговый инвертор*). Обычно используется разбиение полосы на 2 поддиапазона.



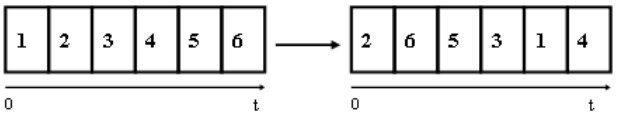
Полосовые скремблеры используют способ разбиения полосы речевого сигнала на несколько поддиапазонов с частотными перестановками этих поддиапазонов. Полосовой скремблер может быть реализован на основе БПФ.

В таком скремблере на передающей стороне производится прямое БПФ, частотная перестановка полос, а затем — обратное БПФ. На приёмной стороне осуществляются аналогичные преобразования с обратной частотной перестановкой полос. В скремблерах с БПФ возможно достичь высокой степени защиты информации за счёт увеличения количества перемешиваемых полос, однако на практике этот метод скремблирования в подвижной радиосвязи применяется редко в связи со сложностями технической реализации. Кроме этого, скремблеры с БПФ вносят в канал связи временную задержку.

Временные преобразования



Временная инверсия. Исходный сигнал делится на последовательность временных сегментов и каждый из них передается инверсно во времени — с конца к началу.



Скремблер с временными перестановками. Речевой сигнал делится на временные кадры, каждый из которых подразделяется на сегменты, подвергающиеся перестановке.

Комбинированные преобразования

Для дальнейшего повышения степени закрытия речи используется комбинация временного и частотного скремблирования. В таком скремблере после аналого-цифрового преобразования спектр оцифрованного речевого сигнала разбивается на частотно-временные элементы, которые затем перемешиваются на частотно-временной плоскости в соответствии с одним из криптографических элементов и суммируются, не выходя за пределы частотного диапазона исходного сигнала.

Динамические (роллинговые) скремблеры

Все рассмотренные выше скремблеры предполагают фиксированные параметры преобразования сигнала (фиксированные ключи) в течение передачи речевого сообщения и поэтому называются *статическими*.

Дополнительное повышение уровня закрытия информации может быть обеспечено изменением параметров преобразования сигнала во времени. Такие скремблеры называются *динамическими*. В современной практике их часто обозначают термином *роллинговые скремблеры*.

Динамические скремблеры, как правило, существенно дороже скремблеров с фиксированными параметрами преобразования сигнала, сильнее влияют на характеристики радиосредств и требуют начальной синхронизации. Однако их применение действительно затрудняет возможности перехвата переговоров, в особенности в реальном масштабе времени. Это объясняется тем, что изменение ключевых параметров во времени теоретически делает возможным резкое увеличение количества ключей, под которыми для роллинговых скремблеров обычно понимают

некоторое значение, определяющее порядок изменения параметров преобразования сигнала. Например, ключом может быть начальное значение генератора псевдослучайной последовательности, в соответствии с которой меняется определенный ключевой параметр.

Временные преобразования сигнала в сочетании с изменением ключевых параметров во времени сложны для реализации и требуют относительно длительной синхронизации, поэтому они пока не нашли свое применение в роллинговых скремблерах. Для способов частотного преобразования сигнала изменяемыми ключевыми параметрами могут быть частота инверсии (для частотного инвертора), частота разбиения полосы сигнала (для полосно-сдвигового инвертора), комбинация частотной перестановки поддиапазонов сигнала (для полосового скремблера). Большинство известных моделей роллинговых скремблеров используют наиболее простой принцип спектрального преобразования — частотный инвертор с изменением частоты инверсии сигнала во времени. Различие скремблеров состоит в числе частот инверсии, скорости их изменения и количестве ключей, определяющих длительность перебора возможных комбинаций изменяемых параметров без их повторения.

Примеры использования

В качестве примера использования скремблирования для обработки звуковых сигналов можно привести аппаратуру ЗАС, например, аппаратура закрытия информации Т-219 «Яхта», предназначенная для закрытия оперативно-речевой информации. ЗАС Т-219 «Яхта» представляет из себя аналоговый синхронизируемый скремблер, принцип работы которго заключается в том, что при речевом обмене, в режиме FSK передается синхропоследовательность, расположенная точно по середине спектра. Сам речевой спектр разбивается на две части, выше и ниже этой последовательности. Все это разбивается на неравные временные отрезки, в пределах которых переставляются местами и инвертируются эти два речевых подканала. Аппаратура ЗАС Т-219 «Яхта» считается скремблером временной стойкости, широко используется для передачи оперативной информации, имеющей ограниченный срок "свежести".

Источники:

1. Скремблер. https://ru.wikipedia.org
2. Скремблеры. http://citforum.ru
3. Основы телекоммуникаций. http://koapp.narod.ru
4. Материалы с сайта http://www.russianarms.ru.
5. Методы защиты информации в системах конвенциональной радиосвязи / А.М. Овчинников. http://www.sagatelecom.ru