Скремблер (англ. 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.

Цели скремблирования

Применительно к телекоммуникационным системам скремблирование повышает надёжность синхронизации устройств, подключённых к линии связи (обеспечивает надёжное 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 перехвата противником. Процесс скремблирования может включать в себя добавление определённых компонент к исходному сигналу либо изменение важных частей сигнала для того, чтобы усложнить восстановление вида исходного сигнала либо для придания сигналу определённых статистических 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.

Типы скремблеров

1. Самосинхронизирующиеся скремблеры (СС)
2. Аддитивные скремблеры (с установкой)

Сравнение скремблеров

Скрамблеры имеют определенные недостатки:

* Оба типа может не генерировать случайные последовательности в соответствии наихудших условий на входе.
* Мультипликативные скремблеры привести к ошибкам умножения во дескремблировании (т.е. одно-битовой ошибки при вводе Дескремблера будет приводить к ш ошибок на выходе, где W равно количество отводов обратной связи скремблера в).
* Аддитивные скремблеры должны быть сброшены с помощью кадровой синхронизации; если это не удается, массовое распространение ошибки приведет, как полный кадр не может быть дескремблируются.
* Эффективная длина случайной последовательности аддитивного скремблера ограничена длиной кадра, который обычно значительно короче период PRBS. Путь добавления номера кадров к кадровой синхронизации, можно увеличить длину случайной последовательности, путем изменения случайной последовательности в соответствии с номером кадра.

Скремблер «GUARD Bluetooth»

Технические характеристики

Принцип кодирования: инверсия звукового спектра;

Беспроводное соединение: Bluetooth;

Формирование ключа: статическое;

Общее количество комбинаций алгоритма: 4 комбинации;

Количество изменений частоты инверсии: 4 частоты;

Длина ключевой последовательности: 16 бит; Канал связи: полный дуплекс; Разборчивость дескремблированной речи: 95%;

Полоса звуковой инверсии: с 280 Hz до 3140Hz;

Наклон предискажений во время скремблирования звукового потока 6dB на октаву;

Диапазон частот инверсии: с 44.336kHz до 184.734kHz;

Выходной импеданс: с 300 по 500 кОм;

Питание: 9В (крона);

Ток потребления мА: 70 мА; Индикация: светодиодная;

С общими принципами работы устройства можно ознакомиться на сайте проекта, цитата: «Защита информации передаваемая по каналам сотовой связи обеспечивается за счет первоначального разрушения спектра речи и ее временной перестановки на передающей стороне (у того абонента, который говорит). Иначе говоря, в эфир выдается перестановленные местами части слов. Подключившиеся к Вашему разговору третьи лица соответственно слушают или записывают именно искаженную не подлежащую разбору речь Однако имеющийся у Второго абонента с тем же режимом шифрования скремблер, является дескремблером, который восстанавливает зашифрованную речь.»

Разумеется, бесполезно пытаться разобрать закодированную речь без дешифратора на «принимающей» стороне. Передающийся по сети звук напоминает некий гибрид человеческой речи и звука коннекта аналогового модема, если кто-то из вас еще помнит эти замечательные устройства.

Для ведения защищенных переговоров необходимы два устройства. Соответственно, и поставляются они парами в общей упаковке. В комплект входит собственно скремблер, проводная гарнитура и блок питания. Существенный минус – разъем для подключения гарнитуры отсутствует и в случае ее поломки придется обращаться в мастерскую. Странное решение, неужели так сделали ради копеечной экономии на стандартном гнезде 2,55 мм?

Габариты изделия назвать скромными нельзя, размер сопоставим с пачкой сигарет. Судя по объему свободного пространства в корпусе, изготовители не ставили перед собой задачу добиться максимальной миниатюрности прибора. Или, не мудрствуя лукаво, использовали более-менее подходящий по размерам готовый пластмассовый корпус, о чем косвенно свидетельствует выштамповка под отсутствующий шильдик. Обсуждать дизайн устройства не приходится, его здесь нет как такового. Функционал в чистом виде, даже головки саморезов не закрыты декоративными заглушками. Хорошо хоть пластик шероховатый и не выскальзывает из рук. Остается утешаться тем, что демонстрировать такой прибор окружающим все равно не придется. Уж если человек платит немаленькие деньги за шифрование телефонного разговора, то вряд ли будет беседовать при свидетелях. Ладно, считатем, что для данного изделия внешний вид вторичен.

Защиты от пыли и влаги не предусмотрено. Корпус выглядит достаточно прочным, но печатная плата ничем не закреплена. Впрочем, ломаться там особо нечему, а царапины и прочие мелкие повреждения внешний вид изделия не испортят.

«Порадовало» отсутствие каких бы то ни было обозначений на переключателях режимов работы и светодиодах. Многие из нас гордятся тем, что легко разбираются во всех нужных функциях телефона даже не открывая «Руководство пользователя», но здесь такой фокус не пройдет. Понятно, что всякие шильдики-гравировки повышают себестоимость продукта, но могли бы хоть карандашом от руки написать. Запомнить назначение трех переключателей – невелик труд, но как-то неправильно это.

В остальном к устройству претензий нет. Да и какие претензии могут быть к девайсу, выполняющему единственную функцию? Проверить надежность шифрования речи не могу, приходится верить на слово разработчику. Который утверждает, что «скремблеры позволяют защититься от любого способа прослушивания сотовых телефонов, в том числе и от специального оборудования, установленного у оператора.»

Аккумулятор емкостью 540 mAh обеспечивает, по утверждению производителя, работу устройства в течение 10 часов. Более чем достаточно, особенно с учетом явно эпизодического характера использования скремблера. Замена источника питания самим пользователем не предусмотрена, для этого придется разбирать корпус. Надо полагать, сочли пару лет жизни аккумулятора достаточным сроком. За это время либо потребность в секретных переговорах отпадет, либо нанятый киллер разберется со сроком жизни самого владельца.

Имеется режим bypass, т.е. возможность отключения/включения шифрования во время разговора. Без этой функции было бы сложно договариваться с собеседником о выборе режима шифрования, который задается двумя двухпозиционными переключателями. Соответственно, имеем четыре возможные комбинации, которые во время защищенного разговора должны совпадать на обоих устройствах.

Из забавных мелочей – строка из раздела «Гарантия» в прилагаемом описании. «Гарантия не предоставляется, если <…> устройство вышло из строя в результате неправильного подключения к сотовому телефону». Теперь вот мучает любопытство: как добиться такого эффекта по каналу bluetooth?

Мобильный Скремблер Avantalk

Технические характеристики:

1. Максимальная дальность связи между блоком MS и телефоном……….. до 3 метров

2. Минимальное расстояние между блоком MS и мобильным телефоном от 0,5 метра

3. Максимальное время заряда LI-ION аккумулятора…………………………до 10 часов

4. Время работы блока MS с полностью заряженным аккумулятором…… до 8 часов

Мобильный скремблер Avantalk обеспечивает защиту информации, передаваемой мобильным телефоном. Скремблеры активно применяются для защиты телефонных переговоров, не позволяя системам радиомониторинга мобильной связи осуществлять «прослушку» по ключевым словам и характерным изменениям интонации голоса. При использовании скремблера Avantalk подслушивание разговора, который ведется по вашему телефону, становится полностью невозможным, независимо от методики перехвата. Подразумеваются любые методы, включая такие, как контроль «у оператора», пассивный перехват в зоне телефона, активный перехват с переключением телефона на «ложную» базу и т.д. Все эти способы прослушивания будут бесполезны, если вы и ваш собеседник включили режим кодирования. Нужно учитывать, чтобы у абонента на другой стороне был аналогичный прибор. Коды шифрования информации у обоих приборов должны совпадать. Достаточно невысокая стоимость скремблера позволяет создать «сеть» среди постоянных партнеров или внутри корпоративной «верхушки» для ведения полностью «закрытых» переговоров в пределах этой сети. Скремблер Avantalk реализован в виде Bluetooth-гарнитуры и подключается к соответствующему смартфону посредством Bluetooth. При подключенном скремблере разговор ведется через встроенный микрофон. Когда вы дозвонились Вашему собеседнику, один из вас включает режим кодирования. В течение нескольких секунд Ваши устройства будут обмениваться первичными данными и устанавливать связь. После установки связи загорится соответствующий светодиод, подтверждающий вхождение в «защищенные режим». После этого Вы можете спокойно беседовать на секретные темы. Голос собеседника в режиме скремблирования несколько искажается. Это нормально, так как сигнал проходит многократную обработку и затем передается по относительно низкокачественному GSM-каналу. Создаваемый дискомфорт не соизмерим с важностью обеспечения конфиденциальности. Для улучшения понимания говорите медленно и разборчиво, а также используйте наушники.

Скремблер для смартфону iProTech FSM-U1

Технические характеристики:

Скремблер реализован в виде гарнитуры и подключается к соответствующему разъему смартфона.

При подключенном скремблере разговор ведется через него или наушники.

FSM-U1 имеет встроенный динамик и микрофон.

Устройство питается от встроенного Li-Pol аккумулятора 3.7В емкостью 290 мАч.

Ресурс аккумулятора – до 2.5 часов разговора в режиме скремблирования.

Время перезаряда – 2 часа, от USB (компьютер, сетевое з/у или разъем в автомобиле).

FSM-U1 — новое устройство кодирования разговоров для мобильного телефона-смартфона. В скремблере реализован новый мощный алгоритм «закрытия» разговора с помощью технологии «многократной динамической обработки фазы». При использовании FSM-U1 подслушивание разговора, который ведется по вашему телефону, становится полностью невозможным, независимо от методики перехвата. Подразумеваются любые методы, включая такие, как контроль «у оператора», пассивный перехват в зоне телефона, активный перехват с переключением телефона на «ложную» базу и т.д. Все эти способы прослушивания будут бесполезны, если вы и ваш собеседник включили режим кодирования.Достаточно невысокая стоимость скремблера позволяет создать «сеть» среди постоянных партнеров или внутри корпоративной «верхушки» для ведения полностью «закрытых» переговоров в пределах этой сети.Скремблер реализован в виде гарнитуры и подключается к соответствующему разъему смартфона. При подключенном скремблере разговор ведется через него или наушники. FSM-U1 имеет встроенный динамик и микрофон.