УДК 621.391(075.8)

Трещев Иван Андреевич
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Россия, Комсомольск-на-Амуре
Заведующий кафедрой «Информационная безопасность автоматизированных систем»
Кандидат технических наук
E-Mail: kalkt@yandex.ru

О подходе к скремблированию цифрового аудиопотока для защиты телефонных переговоров в условиях отсутствия шумов

Аннотация. В данной работе рассматривается проблема скремблирования данных аудио потока в реальном времени при использовании не зашумленного канала. Приведены результаты использования данного метода.

Ключевые слова: информационная безопасность; скремблирование; БПФ; AES256.

Скремблирование и обратные преобразования

Под скремблированием подразумевается преобразование исходного аудио сигнала с целью минимизации признаков аудио данных, в результате которого этот сигнал становится неразборчивым и неузнаваемым. При этом он занимает такую же полосу частот спектра, как и исходный сигнал. Необходимым свойством такого преобразования является возможность обратного преобразования для восстановления речевого сигнала на приемной стороне[1].

При скремблировании возможно преобразование речевого сигнала по трем параметрам: амплитуде, частоте и времени. Однако 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[1].

В данной работе мы применяем полосовой скремблер на основе быстрого преобразования Фурье[2]. В таком скремблере на передающей стороне производится прямое БПФ, частотная перестановка полос, а затем - обратное БПФ. На приемной стороне осуществляются аналогичные преобразования с обратной частотной перестановкой полос. В перестановке полос мы задействуем алгоритм шифрования AES256 в режиме шифрования по счетчику. В нашем случае – ключ скремблера используется для ключа алгоритма AES256, с помощью которого мы шифруем данные полученные от 128 битного счетчика, и в соответствии с полученной шифрованной информацией мы переставляем частоты, полученные в результате быстрого преобразования Фурье[3].

После выполнения быстрого преобразования Фурье единственная проблема - график частот будет симметричен относительно частоты дискретизации сигнала деленной на 2 (проблема зеркальности), что кстати согласуется с теоремой Котельникова[3]. Самый простой способ борьбы с этой проблемой – обнулить часть слева от частоты дискретизации деленной на два, а сигнал справа – умножить в два раза.

Исходя из того, что у нас в качестве сигнала используется речь, а это спектр от 300Гц до 4000Гц[4], соответственно, оптимальной будет дискретизация с частотой 8000Гц, то представляется оптимальным путем проводить БПФ над 1024 отсчетами, получая в итоге 512 полос сигнала, из-за зеркальности спектра. Но так как в результате перестановок 512 полос и передачи их по радиоканалу мы не сможем вычленить частоты обратно из-за шумов – мы переставляем по 16 полос, и итоговый скремблер у нас будет с тридцати двумя полосами.

Существует несколько стандартных режимов шифрования[2]:

1. *Режим электронной кодовой книги (Electronic Codebook, ECB);*
2. *Cipher Block Chaining (Режим сцепления блоков шифротекста, CBC);*
3. *Cipher Feedback (Режим обратной связи по шифротексту , CFB);*
4. *Режим обратной связи (Output Feedback, OFB);*
5. *Режим Счетчика (Counter Mode, CTR).*

Из вышеперечисленных алгоритмов, для скремблирования, был выбран режим счетчика (CTR), с небольшой модификацией, вместо XOR мы выполним перестановку частот по ключу. Режим счетчика – единственный применимый в нашем случае алгоритм из-за того, что мы работаем с аудиоданными, которые могут серьезно повредиться в процессе их передачи, тем самым нарушив обратную связь, присутствующую во всех перечисленных алгоритмах, кроме режимов CTR и ECB. Самый простой способ перестановки по ключу – задание соответствия байтов ключа полосам частот, и простая сортировка байтов ключа методом перестановки.

Дешифрование в этом случае будет выглядеть так: создание копии ключа, сортировка ключа, задание соответствия байтов сортированного ключа полосам частот, перестановка частот в соответствии с исходным ключом (неизмененной копией). При данном алгоритме могут возникать коллизии при совпадении байтов ключа, но так как наша цель – получение распознаваемого аудио сигнала содержащего речь, а данные коллизии будут достаточно редкими, то можно игнорировать эту особенность данного алгоритма. Для данного режима шифрования (CTR) мы выбрали хорошо зарекомендовавший себя алгоритм AES256, в частности из-за того что он прост в реализации, и многие современные процессоры скремблеров имеют аппаратный модуль шифрования данным алгоритмом.

Результаты эксперимента

Спектр типового сигнала речи(амплитудно-частотная характеристика сигнала с распределением по времени) представлен на рисунке 1. На нем мы можем хорошо различить аудиоданные.

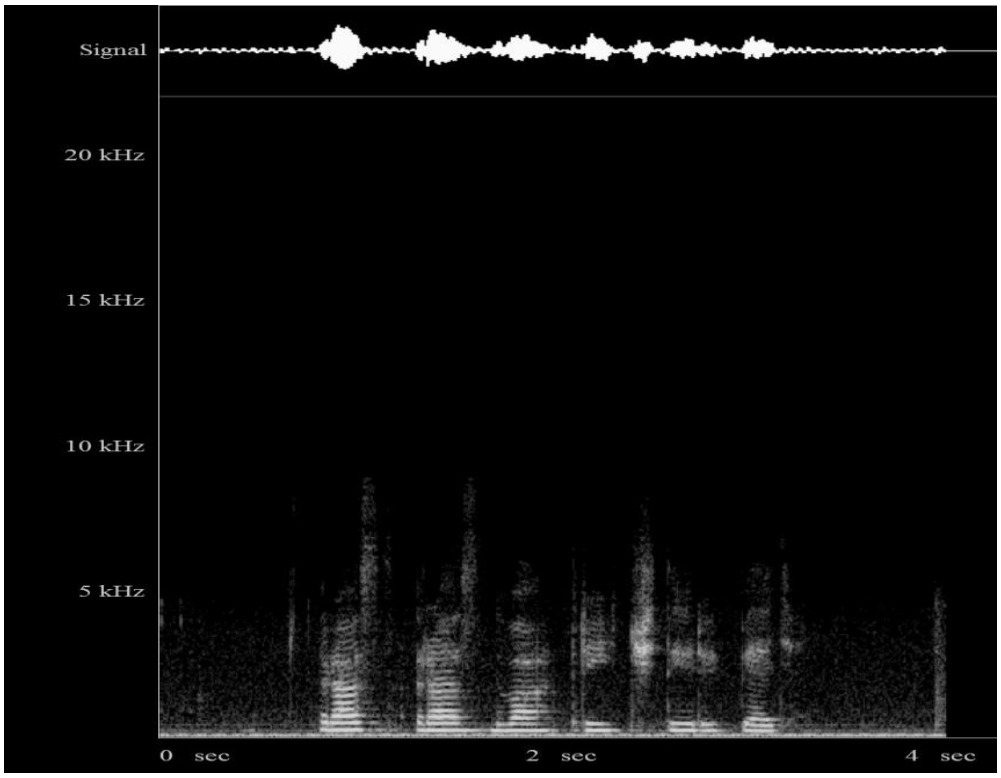

Рис. 1. *Спектр исходного сигнала*

Спектр скремблированного сигнала представлен на рисунке 2. Как можно заметить – аудиоинформация совершенно неразличима.

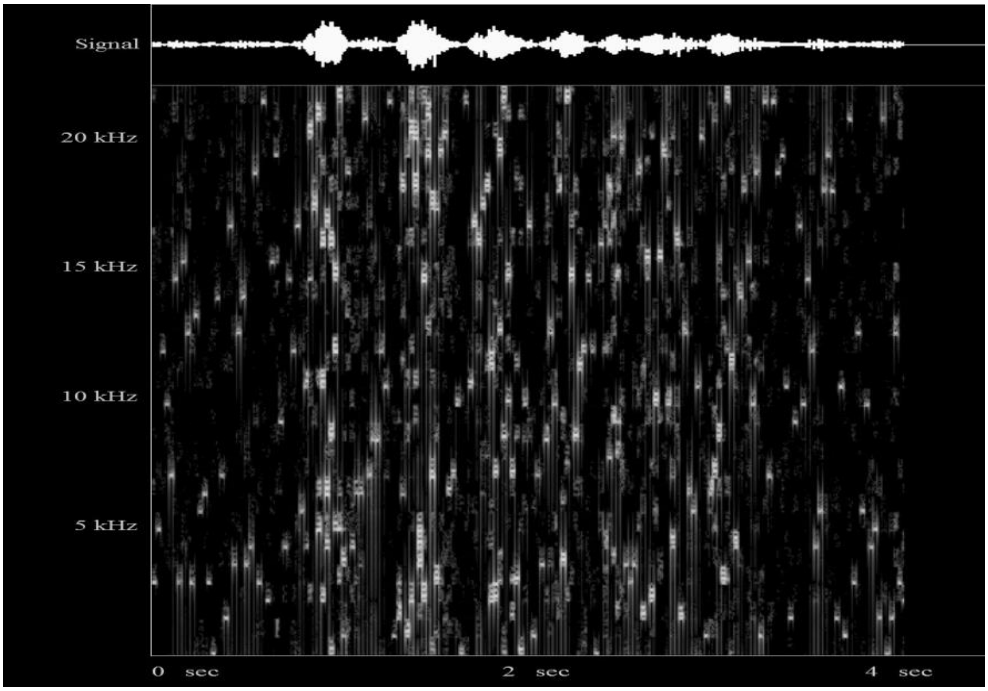

Рис. 2. *Спектр скремблированного сигнала*

Спектр расшифрованного сигнала представлен на рисунке 3. Спектр исходного сигнала восстановлен, хоть и с небольшими потерями.

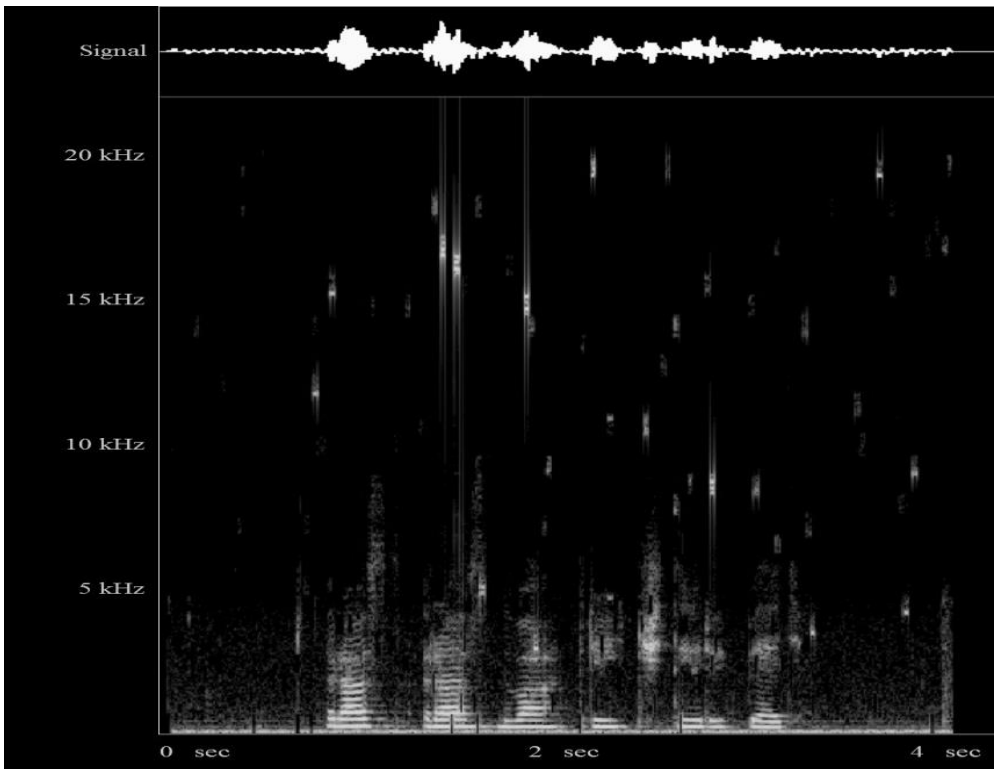

Рис. 3. *Спектр расшифрованного сигнала*

Заключение

Приведенный в работе подход к скремблированию аудио потока позволяет получить зашумленный спектр информативного сигнала, поддающийся восстановлению на приемном конце. Следует отметить, что при использовании каналов связи с высоким уровнем шумов предложенный метод не применим, поскольку в данном случае наблюдается существенный вклад информативного аудио сигнала в результирующий спектр скремблированного сигнала.

ЛИТЕРАТУРА

1. **Сергиенко, А.** Цифровая обработка сигналов / А.Б. Сергиенко – М.. Изд-во: «Питер», 2003. – 408с.
2. **Рабинер, Л.** Теория и применение цифровои обработки сигналов/Л. Рабинер, Б. Гоулд – М.: Изд-во «Мир», 1996. – 848с.
3. **Блеихут, Р.** Быстрые алгоритмы цифровои обработки сигналов/ Р. Блеихут, 1989. – 428с.
4. **Даджион, Д.** Цифровая обработка многомерных сигналов/Д. Даджион, Р. Мерсеро – М.: «Мир», 1988. – 488с.

Ivan Treschev
Komsomolsk-on-Amur state technical University
Russia, Komsomolsk-on-Amur
E-Mail: kalkt@yandex.ru

On the approach to digital scrambling audio stream to protect telephone conversations in the absence of noise

Abstract. In this paper we consider the problem of data scrambling of the audio stream in real time using not noisy channel. The results of using this method.

Keywords: information security; scrambling; FFT; AES256.

REFERENCES

1. Sergienko, A. Cifrovaja obrabotka signalov / A.B. Sergienko – M.. Izd-vo: «Piter», 2003. – 408s.
2. Rabiner, L. Teorija i primenenie cifrovoi obrabotki signalov/L. Rabiner, B. Gould – M.: Izd-vo «Mir», 1996. – 848s.
3. Bleihut, R. Bystrye algoritmy cifrovoi obrabotki signalov/ R. Bleihut, 1989. – 428s.
4. Dadzhion, D. Cifrovaja obrabotka mnogomernyh signalov/D. Dadzhion, R. Mersero – M.: «Mir», 1988. – 488s.