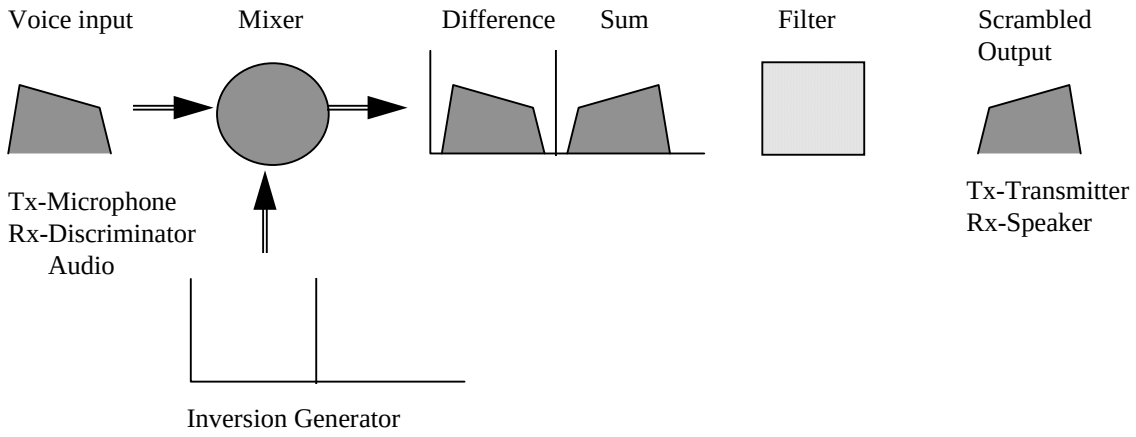
Scrambling Technical Overview

By Ken Beckwith
Applications Engineer

Scrambling is the process by which audio signals are altered to make them unintelligible to listeners who are not the intended recipients of the communication. There are many different techniques used to perform this function. Our purpose is not to describe the various types but to introduce the scrambling method Transcrypt International uses. That process is called frequency inversion. This process alters the frequency of the signal so it is not understandable. Simple inversion is fairly easy to decode and is not a highly secure method of scrambling but variations of inversion can make the process significantly more difficult to decode, thus the security of the method increases drastically. Transcrypt uses simple inversion and several variations to offer several levels of security depending on the need of the user.

The process of inversion is actually quite simple. The audio signal is fed into a mixer along with an inversion frequency, usually an audio tone located at the upper end of the audio spectrum. The mixing process produces a signal consisting of the sum of the two input signals and the difference of the two input signals. The two original signals are absent from the output in a properly balanced mixer. The sum component is then filtered out, leaving only the difference. The range of frequencies in this signal is roughly the same as the original signal, but the content is vastly different. The low frequencies of the original signal become high frequencies and the high frequencies of the original signal become low frequencies. This difference signal, which is very difficult to understand, is transmitted as the scrambled audio.



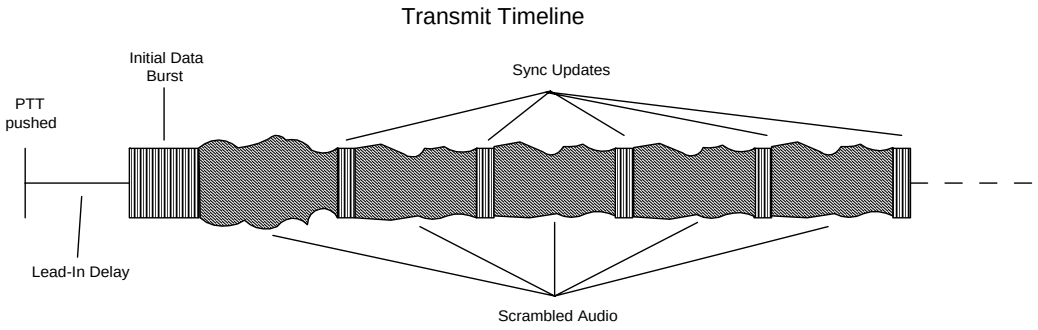
The process of scrambling by frequency inversion is a balanced process, which means that the process of descrambling is identical to the scrambling process. When clear audio is fed into the scrambler, the output is scrambled. When scrambled audio is

input, the result is clear, or descrambled audio. As a result of extensive filtering and other factors, the quality of the decoded signal usually is not quite as good as the original, but is recognizable and intelligible. The listener can understand what is being said and is able to recognize the speaker.

Since a signal scrambled with a simple inversion frequency is easily decoded and recovered, methods are employed to make the signal more secure. Varying the inversion frequency increases the difficulty of decoding since the decoder must also follow the varying inversion frequency. If it varies slowly, this is not too difficult, but if the frequency varies quickly, the difficulty increases tremendously. If the frequency varies on a linear basis, it is referred to as a rolling code. If it varies on a psuedo-random basis, it is referred to as a hopping code.

When rolling or hopping code scrambling is used, the receiving and transmitting scramblers must be in synchronization or the signal will not be decoded properly. In Transcrypt scramblers, the transmission of data is used to signal the receiving scrambler to begin decoding and to keep the scrambler in sync.

The transmitting scrambler sends a packet of data at the beginning of a transmission to signal the receiving scramblers. The data is delayed a few hundred milliseconds after PTT in order to allow the receiving radios to open audio signal paths so the data can be received. This data contains necessary information about the scrambled signal which the receiving scrambler uses in decoding. Other information pertinent to optional features in the scrambler is also sent.



Periodically (about every half second), another shorter burst of data called a sync update is sent to synchronize the receiving scramblers with the transmitter. When transmission stops, data also is no longer sent, and the receiving scrambler drops out of decode mode after failing to receive two scheduled sync updates. Any time the receiving scrambler misses two sync updates is a row, it will drop out of sync and discontinue decoding. This is how the receiving scrambler knows that scrambling has ceased.

The SC20-460 series scramblers have many other features besides scrambling. They are part of a larger control system we have named TCAD (Transcrypt Computer Aided Dispatch). As part of this system, they are capable of ANI (Automatic Number Identification), status reporting, Emergency, Selcall (paging), OTAR (Over The Air Reprogramming) and Kill and Revive. These features make the scramblers quite versatile, and understanding and implementing these features can be somewhat complex. To avoid confusion, information on these features is included in other documents.

The inclusion of data into the scrambled signal affects the way the radio works. When data is being transmitted and during the initial delay before data is transmitted, the user's voice audio is blocked and cannot be heard in the receiving radio. This happens primarily at the beginning of the transmission. Because of this the user must be aware that once PTT is pushed, he must wait for a second or so before speaking to allow time for the data to be transmitted. Sync updates are of such a short duration that they present very little effect on speech even though they occur regularly. The interruption can be heard but is very insignificant.

Each person using a scrambled radio must also be careful to observe good radio protocol and monitor the channel before using it. If a transmission is interfered with, such as when someone steps on someone else's transmission, the sync update data is corrupted and the receiving scramblers will lose sync. Once sync is lost, the scrambler will not decode until the next transmission, when an initial data burst is sent.

The same result will occur if the receiving radio loses the signal for a brief period of time. If the scrambler does not decode two sync updates in a row, the scrambler drops out of sync and the rest of the transmission is lost.

The range performance of the radios will also be affected by the scrambler. Any noise being received will be decoded along with the audio and will be changed in frequency and increased in level. This produces an apparent loss of range. The RF performance of the radio is not affected but audio noise is changed and increased as a result of the scrambler decoding noise. Filters can be added to the radio to decrease this effect although some radios already have filters incorporated into the radio circuitry.

Although the scrambler does affect radio performance, the effects are not significant in most cases. The user must realize that security does come at a cost and that a balance must be achieved between system performance, audio quality, security and cost. It is Transcrypt's goal to provide the highest quality equipment at a reasonable price. Our training provides thorough preparation to equip the user and maintenance provider with the tools needed to insure that optimum performance is achieved.

