Selected Comments on Scrambler Security

James E. Gilley
Chief Scientist
Transcrypt International, Inc.
jgilley@transcrypt.com

September 16, 2003

1 Introduction

Analog scramblers provide an acceptable level of communications security for many applications; however, the specific level of security these scramblers provide is nearly impossible to precisely quantify. Most users of scramblers have little choice but to believe whatever their vendor tells them about the security level provided, which is invariably 'the best in the industry'. What users really need is an objective and unbiased measure of the true level of security provided by scramblers.

In this paper, I will explore the issue of communications security, investigate the security provided by analog scramblers, discuss cryptanalysis and other forms of attack, and describe the security-relevant aspects of Transcrypt's scramblers. My goal is to provide the reader with the knowledge required to judge whether or not an analog scrambler is appropriate for a given application.

2 Communications Security

What does 'communications security' mean? In the context of this paper, I define communications security to be synonymous with privacy. A scrambler achieves communications security if the scrambled conversation remains private amongst the parties who are authorized to participate in this conversation. If an adversary or eavesdropper is able to intercept the scrambled communications and obtain information about its contents, then the scrambler has failed to provide communications security.

2.1 Information Value

Clearly, the information contained in a scrambled conversation must have some inherent value, otherwise the conversation would not need to be scrambled. Before you can determine the security provided by a scrambler, you must consider the value of the information the scrambler is intended to protect. The value of information is determined primarily by the potential for damage should this information fall into the wrong hands. Furthermore, the value of information usually, though not always, decreases with the passage of time. An example may help to clarify these points.

Suppose the information is a tactical battle plan for a platoon of soldiers. This plan needs to be communicated, then executed. If the enemy discovers the battle plan, the outcome of the battle may change. Obviously, the battle plan has substantial value, since the outcome of the battle may depend on the confidentiality of the information. However, once the battle has concluded, the value of the information is greatly diminished, since it is now too late to affect the outcome of the battle.

2.2 Securing Information According to its Value

Since the value of information depends both on the potential for damage if the information falls into the wrong hands, and on the length of time for which the information remains sensitive, the level of security used to protect the information must be based upon these two criteria.

Information having little value need not be protected to the same extent as information having great value. Likewise, information which loses its value very rapidly can be afforded less permanent protection than information which holds its value for a long period of time. The more valuable the information, and the longer the information remains valuable, the greater the level of security needed to protect it, and the greater the expense and difficulty of providing this protection.

In theory, most forms of communications security can be compromised by an adversary having infinite time and resources. The relevant question to consider is this:

> Can an adversary recover useful information from secure communications within the time this information remains valuable?

The answer to this question depends on the technique used to secure the information.

2.3 Options for Providing Communications Security

The options available for providing communications security are numerous and diverse. On the low end, devices such as simple fixed-frequency inversion scramblers provide a strictly minimal level of privacy from some casual eavesdroppers. On the high end, classified communications systems costing many millions of dollars protect national security assets from foreign intelligence agencies. Most communications require a level of security somewhere between these two extremes.

Two-way land mobile radio users have historically had two options for communications security: analog scrambling, and digital encryption. Analog scrambling applies some form of analog transformation to voice in order to render it unintelligible. Scrambled voice is still an analog audio signal, though it may not sound much like voice. Digital encryption converts analog voice into a digital signal, then digitally encrypts this signal with a cipher. Encrypted voice is digital information that must somehow be sent across the analog radio channel.

2.3.1 Distinguishing Analog Scrambling from Digital Encryption

Determining whether a specific device uses analog scrambling or digital encryption can be difficult and confusing. Some analog scrambling is implemented using digital signal processing. This means the audio is converted to a digital signal, manipulated digitally, then converted back to analog. Most digital encryption converts the encrypted digital voice back to an analog signal so that it can be transmitted over the analog communications channel. So the question is:

> Does this device use analog scrambling or a digital encryption?

The key to distinguishing between the two is the technique used to secure the voice.

If the technique used to secure the voice only involves some manipulation of the time or frequency characteristics of the speech signal, the device uses analog scrambling. If the technique used to secure the voice involves encrypting digitized voice with a conventional cipher algorithm to yield digital ciphertext, the device uses digital encryption. By these definitions, the Motorola DES product uses digital encryption, whereas the Transcrypt SC20-DES uses analog scrambling.

A further clue, and one that is easy to obtain, is what the 'secure' voice sounds like when intercepted from the radio channel. If the signal sounds like static, the device uses digital encryption. If the signal does not sound like static, the device uses analog scrambling.

3 Analog Scramblers

Analog scramblers provide an acceptable level of communications security for many situations. Although they are not suitable for use with information that is extremely valuable for a long period of time, they are more than adequate for protecting tactical communications that do not involve life-or-death consequences. Some analog scramblers provide a greater degree of communications security than others, but *all* analog scramblers have an upper limit on the security they are capable of providing. I will explore that issue in greater detail later in this paper.

3.1 Frequency Inversion

Analog scramblers may alter the audio signal in the time domain, the frequency domain, or both, using any number of analog or digital signal processing techniques. Many popular scramblers alter the signal in the frequency domain, using a technique known as frequency inversion.

Frequency inversion alters the audio by changing its frequency spectrum to a mirror image of the original, or in other words, low frequencies become high frequencies, and vice versa. This renders the audio unintelligible to normal listeners.

Frequency inversion is a modulation process where the original audio is modulated with a carrier at the inversion frequency. The audio is usually filtered before and after inversion. If the process is done correctly, it can be reversed by applying the same process to the inverted audio, producing a replica of the original audio.

3.1.1 The Range of Useful Inversion Frequencies

Audio signals used in two-way land-mobile radio communications must be filtered to limit their frequency spectrum to be compatible with the radio channel. Most radios preserve audio in the range from 300 Hz to 3 KHz, and eliminate audio outside this frequency range. Due to this filtering, the range of useful inversion frequencies is limited. If the inversion frequency is too low, the scrambled signal will suffer from aliasing, where part of the inverted spectrum folds back upon itself, irreversibly destroying that portion of the spectrum in the process. If the inversion frequency is too high, the resulting inverted spectrum will be outside the passband of the filters, again irreversibly destroying that portion of the spectrum.

3.1.2 The Effective Difference between Two Inversion Frequencies

If audio inverted with one inversion frequency is recovered with a different inversion frequency, the result will not be the same as the original clear audio. However, if the two inversion frequencies are close, the recovered audio will be intelligible. In order to provide a useful amount of privacy, two inversion frequencies must differ by an amount great enough so that the audio scrambled by one is not intelligible when recovered by the other. The amount these inversion frequencies must differ in order to provide privacy depends on the skill of the person listening to the recovered audio, and cannot be precisely specified.

3.1.3 The Number of Useful Inversion Frequencies is Small

Since the range of inversion frequencies is limited by the filters used in two-way radios, and since two inversion frequencies must differ by a certain amount in order to be distinct, only a small number of inversion frequencies are truly useful for analog scrambling. This makes it much easier to attack a frequency inversion scrambler than some marketing literature might lead you to believe. Claims of hundreds of possible inversion frequencies are meaningless.

3.2 Rolling Code Scrambling

Historically, fixed-frequency inversion was used to provide voice privacy. The problem with fixed-frequency inversion is that it is very easy for an adversary to recover the clear audio, since the inversion frequency is constant. A solution to this problem is to vary the inversion frequency over time, in a way that is difficult for an adversary to track.

A rolling-code frequency inversion scrambler alters audio signals using frequency inversion, but the inversion frequency changes with time. Most rolling code scramblers have a finite set of discrete inversion frequencies. At any given moment in time, they invert the audio using one of the frequencies from this set. As time passes, the scrambler will select a new inversion frequency from the set. Several different techniques are used to change the inversion frequency over time. All require timing synchronization between the transmitting and receiving scramblers, so that the changes in inversion frequency are made in unison at both ends.

3.2.1 Frequency Hopping

One way to change the inversion frequency over time is to hop it from one value to another. A hopper chooses a particular inversion frequency, inverts the audio for some period of time using this frequency, then chooses a new inversion frequency, and repeats this process. Each time the inversion frequency changes, the new frequency can be any of those in the overall set of inversion frequencies. In this way, the present inversion frequency is not constrained by the previous inversion frequency. Figure 1 shows a plot of the inversion frequency as a function of time for a typical frequency hopping inversion scrambler.

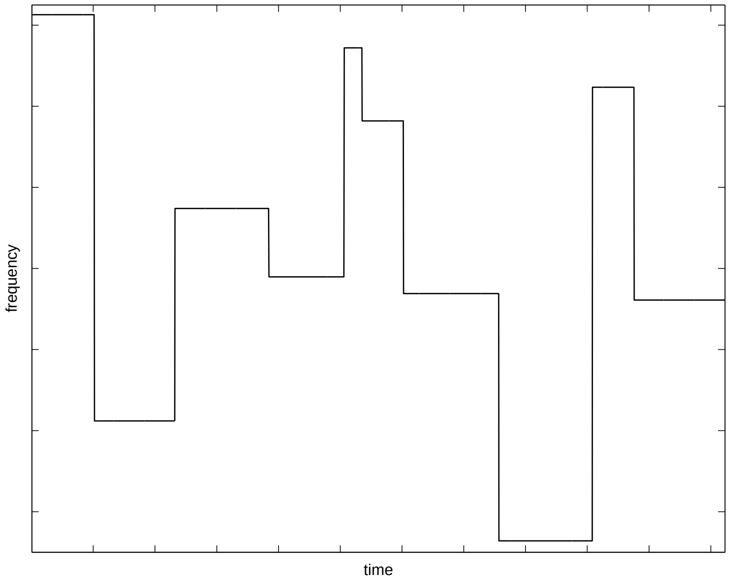

Figure 1: Frequency Hopping Inversion

A problem with random frequency hopping is that it cannot be done very rapidly. Whenever the inversion frequency changes from one value to another, the recovered audio will suffer degradation. The larger the difference between the two inversion frequencies, the worse the degradation. In practice, the hopping rate is limited to about ten times per second or less, due to audio quality issues.

3.2.2 Frequency Sweeping

Another way to change the inversion frequency over time is to sweep it between upper and lower limits. A sweeper starts out at one limit, then progressively changes the inversion frequency in the direction of the other limit. It continues this process until the opposite limit is reached, then it reverses the direction of the change, and continues back to the first limit. Each time the inversion frequency changes, the scrambler chooses an inversion frequency immediately adjacent to the previous inversion frequency. This way, each frequency change is very small. Figure 2 shows a plot of the inversion frequency as a function of time for a typical frequency sweeping inversion scrambler.

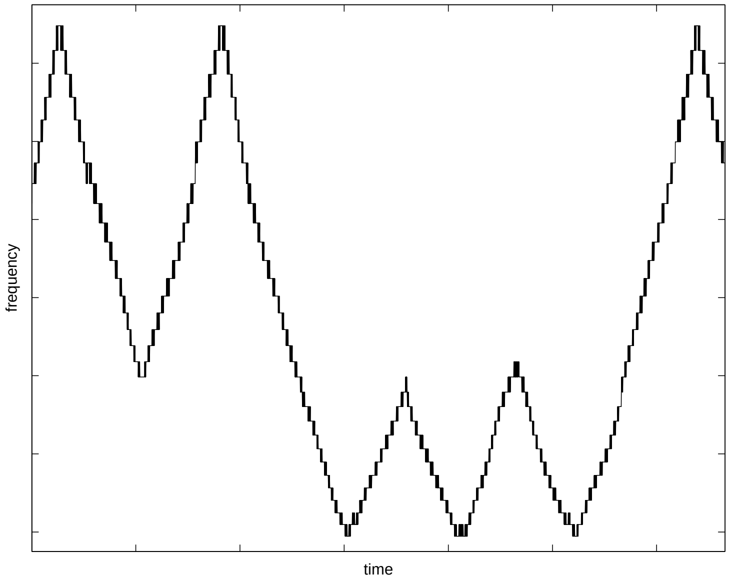

Figure 2: Frequency Sweeping Inversion

The advantage of frequency sweeping is that since each individual change is small, the time between changes can be very short. The net result is that the inversion frequency changes by a large amount over a relatively short period of time, but does so in a continuous manner. The audio degradation is minimal, while the scrambled audio is highly unintelligible.

Regardless of whether a rolling code scrambler uses hopping or sweeping, it must have a way of making the changes to the inversion frequency in a deterministic manner. If this were not the case, the receiving scramblers would not be able to recover the scrambled audio; however, the changes must be done in a manner that is unpredictable by an adversary.

3.3 Making Scramblers Secure

In order to be useful and effective, a rolling code scrambler must alter its scrambling as a function of time, and also as a function of a secret value, or code. The code is a secret value chosen by the user, analogous to the secret key of a cipher. All scramblers that are to communicate with each other must have the same code. This code must be kept secret, since any adversary who discovers the value of the code can intercept scrambled communications by obtaining a compatible scrambler and loading it with the proper code.

3.3.1 The Number of Codes

To be secure, the scrambler must provide a large number of codes. If the scrambler only allowed a small number of codes, an adversary could simply try all the possible codes. Furthermore, if the same type of scrambler is sold to many different customers, there must be enough codes to prevent two different customers from selecting the same code by chance. However, if one model of scrambler provides more codes than another model, it does not mean the former is more secure than the latter. Having more codes only makes it more difficult to perform an exhaustive search of the codes. Later in this paper, I will discuss why this is never the most effective way to attack a scrambler.

3.3.2 Cryptographic Building Blocks

Most scramblers use some elements of cryptography as building blocks. A rolling code scrambler must somehow generate time-varying scrambling that is a function of a secret code. One way to do this is to utilize a pseudo-random number generator to create a code-dependent sequence of numbers that can be used to control the scrambling. The field of cryptography offers extensive possibilities for creating pseudo-random number generators. Some scramblers use linear feedback shift registers (LFSRs) as pseudo-random number generators. LFSRs have well known mathematical properties that make them ideally suited to generating code-dependent pseudo-random sequences. However, these properties also make them vulnerable to cryptanalysis, as I will discuss later in this paper.

3.3.3 Randomization

A rolling code scrambler requires some form of randomization so that the scrambling is different for each message. If the scrambling depended only on the secret code, then each time a user operated the scrambler, the scrambling would be the same. This is creates a weakness that should be avoided.

4 Cryptanalysis

The goal of cryptanalysis is to recover information from secure communications, or in other words, to break the scrambling or encryption. Since the focus of this paper is rolling code frequency inversion scrambling, I will concentrate on those aspects of cryptanalysis most applicable to these scramblers.

4.1 Avenues of Attack

Rolling code frequency inversion scramblers may be attacked in two fundamental ways. In the first way, I view the scrambler as a classic cipher, and I attempt to use the techniques of classical cryptanalysis to uncover some weakness in the cryptographic underpinnings of the scrambler. In the second way, I view the scrambler as an audio processor, and I attempt to use signal processing to restore intelligibility to the scrambled voice. Both techniques are equally valid, and may be used either alone or in combination.

4.2 Classical Cryptanalysis

Classical cryptanalysis attempts to break a cipher by utilizing statistics, mathematics, and analysis. Generally, the cryptanalyst searches for a weakness or vulnerability in the cipher, or in the way in which the cipher is used. The cryptanalyst is assumed to have access to the ciphertext and the cipher algorithm itself. Only the plaintext and the secret key are unknown to the cryptanalyst, and recovering these is the goal of cryptanalysis. Since most analog scramblers use some form of a cipher as a building block, it may be possible to attack a scrambler using some sort of classic cryptanalysis.

The obvious target of cryptanalysis is the scrambler's pseudo-random number generator. By definition, the output of this generator is not truly random, but is instead dependent upon the user's secret code, and the algorithm used in the generator. Additionally, all pseudo-random number generators produce a sequence of numbers that will eventually repeat. A cryptanalyst will look for weakness in the way the pseudo-random number generator operates, and will also attempt to exploit any repetition which may occur in the output sequence.

The major difficulty in attacking the scrambler's pseudo-random number generator is obtaining access to the output sequence. Most scramblers do not directly generate an inversion frequency from the pseudo-random number generator. Instead, the pseudo-random sequence is fed to an algorithm that creates an inversion frequency based not only on the sequence, but also on other factors, such as whether the scrambler is hopping or sweeping. While not a cipher per se, this frequency generation algorithm is also subject to attack. Ultimately, the cryptanalyst will attempt to recreate the inner working state of the scrambler based on whatever external observations are available.

A final obstacle to cryptanalysis is the secrecy of the scrambler design. A worst case assumption is that the cryptanalyst knows every last detail of the scrambler design; however, in reality, this is almost never the case. Without knowing the design of the pseudo-random number generator or the scrambler algorithm, cryptanalysis is essentially hopeless. Therefore, while not entirely impossible, classical cryptanalysis is likely to be an adversary's last choice in attacking a frequency inversion scrambler.

4.3 Signal Processing

Regardless of how it is designed, all rolling code frequency inversion scramblers use frequency inversion as their basis for providing security. If an attacker can exploit some fundamental limitation of frequency inversion, then cryptanalysis is unnecessary.

Speech has well known statistical properties that are commonly exploited in vocoders to achieve compression. Frequency inversion preserves these properties, but in a manner that is unintelligible to the human ear. Since the statistical properties of speech are still present in scrambled speech, an attacker can use signal processing techniques to determine the statistics of the scrambled audio, then attempt to calculate the inversion frequency. This form of attack is far more likely to succeed than a cryptanalytic attack, and it does not require any knowledge of the scrambler design.

Signal-processing-based attacks can be made in several different ways. If the audio is bandpass filtered prior to scrambling, as it almost always is, the shape of the spectrum of the inverted audio will reveal clues as to the inversion frequency. These clues can be located by performing a fast Fourier transform (FFT) on the scrambled audio. Furthermore, since there are relatively few inversion frequencies available, an attacker could simply try all possible inversion frequencies, then choose the one that is closest to being correct, based on knowledge of the statistics of clear speech.

Signal processing attacks may not be able to recover the user's secret code, but if they are able to provide intelligible audio from a scrambled signal, the scrambler has been broken. Furthermore, even if such an attack is not possible in real-time, given sufficient time and resources, it will most likely succeed. For this reason, all rolling code frequency inversion scramblers have the same upper limit of security, regardless of how many codes they offer, or whether they sweep or hop. Furthermore, the number of keys, or how often they are changed, has no effect on the success or failure of a signal processing attack.

5 Transcrypt Scramblers

In this section, I describe some specific properties of Transcrypt scramblers, and offer some comments about the security provided by these scramblers.

5.1 SC20-460

The SC20-460 is a rolling-code frequency inversion scrambler that uses the sweeping technique described in 3.2.2. The sweep algorithm of the SC20-460 converts a sequence of pseudo-random numbers into a set of time-varying inversion frequencies, which are a function of the secret code. The SC20-460 includes a randomizing element in each transmission, so that the time-varying pattern of the inversion frequency differs from one transmission to the next, even when the code remains the same.

The SC20-460 has a 32-bit scramble code, of which 24 bits are cryptographically significant, and a 32-bit master code, of which approximately 30.6 bits are cryptographically relevant. Therefore, the total number of codes that can affect the scrambling is $2^{54.6}$, or about 27 quadrillion. This is most definitely enough to prevent exhaustive search attacks, and to reduce the likelihood of two customers using the same code to nearly zero.

5.2 SC20-DES

Like the SC20-460, the SC20-DES is also a rolling-code frequency inversion scrambler. However, the SC20-DES uses digital signal processing to avoid aliasing and filter losses, and is therefore able to use a much wider range of inversion frequencies than the SC20-460. The SC20-DES uses a sweeping technique similar to that of the SC20-460, but unlike the SC20-460, the SC20-DES obtains its pseudo-random number sequence from the DES cipher operating in 64-bit output feedback mode. Since the DES cipher has a 56-bit key, the SC20-DES scrambler offers 2^{56}, or about 72 quadrillion codes, slightly more than the SC20-460.

6 Conclusion

Rolling code frequency inversion scramblers provide an acceptable level of communications security for many different applications. However, before choosing any form of communications security, one must understand the value of the information to be protected, and the duration for which the information remains valuable. Scramblers are suitable for non-life-critical, short-term tactical information.

Transcrypt's SC20-460 and SC20-DES scramblers provide the right combination of variables to make cryptanalysis unfeasible, and signal processing attacks difficult. Therefore, I conclude that the SC20-460 and SC20-DES are as good as any scrambler in their class, and should be acceptable in any application where analog scrambling is suitable for the type of information being protected.