CRYPTO 81 Scrambling and Randomization

Subhash C. Kak

Department of Electrical and Computer Engineering

Louisiana State University

Baton Rouge, LA 70803

Summary

This paper is a review of some recent developments in analog signal encryption. We identify the situations which call for analog encryption as against digital encryption. Certain inherent difficulties with using analog encryption over the usual analog channel have been discussed. We also review the rank correlation approach to the properties of specific permutations and describe a few families of permutations which could be used in practical systems.

The essential difference between analog and digital encryption is that in the former the transmission medium is an analog channel with the same bandwidth as that of the signal. This rules out the use of such algorithms in analog encryption that operate on digital codes of the waveforms like PCM, ADPCM or their transforms as in compressed digitized waveforms. For data rate of 60 kb/s and an encryption delay of 5 ms this implies a block size of 300 bits, for which computationally secure ciphers can be designed. The transmission of such ciphers requires a digital channel, however. If the scrambled bits were converted back into analog form and transmitted over the analog channel, the system performance would be highly susceptible to any transmission error or distoriton.

This is because the scrambled analog waveform via digital encryption represents a non-linear transformation creating large high frequency components which are more susceptible to distortion and noise. Such a technique gives poor speech quality over a high-grade telephone line and unacceptable performance for mobile radio. On the other hand if a digital channel were used for transmission one has to pay a price in terms of cost and complexity owing, in part, to large transmission bandwidth requirements. For systems already using digital links the techniques of digital encryption would, however, be justified. The use of these algorithms for other analog applications would not be appropriate, unless one were using several analog channels to transmit the higher rate digital code data.

Analog encryption algorithms may be classified into two broad categories. First we have the techniques of spectrum and time-segment scrambling as also those of masking and transform-domain (where the transforms are linear orthogonal so as not to cause increase in noise) scrambling. The performance of transform-domain scramblers is generally superior to that of time-segment scramblers since the transform domain samples are generally much less correlated. The second category of these algorithms reduce the data rate associated with the signal so that the analog channel can be used for the transmission of the scrambled symbol sequence. The data rate reduction may be accomplished by machine recognition of primitives, such as words in speech, or by standard data compression techniques. The transmitted symbols must be error control coded to correct for errors that might take place in the channel. If a recognition system is used then the redundancy of written text may make such error control superfluous, however. Current recognition

systems are very expensive and work with severely limited vocabularies. Likewise speech data compression schemes operating at rates low enough for use in analog scrambling are in an experimental stage of development. These implies that the techniques of category two are not yet practical but may become so in a few years.

Historically, the first patented scrambler (1881) switched speech rapidly between two or more transmission lines. This was not very effective because of the great redundancy in speech. The next development was frequency inversion of speech which is ordinarily quite unintelligible. In addition to the disadvantage of having a single key associated with it, it was soon found that operators could be trained to directly comprehend such speech. Band splitters were proposed next. In one system the speech band is split into five sub-bands which are then rearranged into new positions with or without inversion. This provides for a total of $5! \times 2^5 = 3840$ keys. But since inversion is not by itself very effective, the total number of usable keys reduces to about 12, which can be quite easily cryptanalyzed.

Time domain scramblers have also been extensively analyzed. These permute speech samples in blocks. Permuting both time and frequency segments simultaneously produces a two-dimensional scrambler. If the block duration is of the order of a few seconds, these scramblers are very secure. For smaller block durations of the order of milliseconds the security is greatly reduced.

Since practical considerations of providing a guard band for easy recovery of the signal demand oversampling, it appears bandwidth expansion would be a problem unless one of the following two techniques are used. First, transform the oversampled signal

sequence block using a basis which is bandlimited to the signal bandwidth, scramble the sequence in the transform domain and perform an inverse transformation before transmission. Second, oversample the signal, scramble, pass through a lowpass filter with cutoff at the expanded signal bandwidth, oversample again and transmit.

An example of the first technique is the transform-domain scrambler, based on prolate spheroidal sequences. It appears, however, that the stringent requirements of channel equalization and descrambler synchronization do not make such a prolate-spheroidal sequence based scrambler to be a very robust system.

Sub-optimum systems that cause bandwidth expansions to remain within acceptable limits have been proposed by Weinstein and Chow and Lee.

Transmission Impairments

These impairments are caused by channel noise and channel distortion. Standard techniques of signal-to-noise ratio enhancement may be used to reduce their effect. To facilitate adaptive equalization one may periodically substitute discrete-level samples for analog samples. This procedure would itself cause some error, however.

Synchronization

This is especially important in transform-domain scrambling where the samples may have very little correlation. In general, effects of lack of synchronization of samples as well as samples blocks need to be investigated for each technique. Earlier studies indicate that the performance is not effected noticeably by small

delay in synchronization for time-domain scrambling. For transform-domain scramblers that performance depends on the transform used.

Families of permutations

Once the analog signal has been put in the appropriate format, say by means of a suitable linear transformation, the next requirement is to scramble its samples by a random permutation. The permutation applied should have as little 'closeness' with the original order as possible.

The 'closeness' between 2 permutations may be measured by means of rank correlation. The two most frequently used rank correlation coefficients are the Spearman's and Kendall's coefficients. Using Kendall's coefficient one can also generate a random sequence of permutations.

The discrete exponentiation function

The mapping $c = m^e \bmod n$ generates a permutation that is at the basis of several cryptographic schemes including the RSA algorithm as well as the Diffie-Hellman key distribution method. It is suggested that since most natural numbers have different first digit probabilities a relationship between the statistics for the first digits at the input and the output of an exponentiator mod n could have considerable significance for cryptanalysis. Experiments on $n < 1000$ show that for many choices of e and n a significant correlation indeed exists for these first digits.

References

[1] S. C. Kak, "Scrambling and randomization", Tech. Report EE 606 Louisiana State University, June 1981.

[2] S. C. Kak, "New results on the first digit problem", Tech. Report EE 607, Louisiana State University, August 1981.

[3] S. C. Kak, "An overview of analog signal encryption", to be published.