

Some Thoughts on Speech Encryption

Aaron D. Wyner
Bell Labs

Abstract—The problem of scrambling a discrete-time analog sequence for the purpose of privacy encoding is studied. A large family of linear orthogonal invertible scrambling transformations is described that result in a negligible expansion of bandwidth and can therefore serve as building blocks in a secure communication system.

IN THIS PAPER we study the problem of scrambling a discrete-time analog sequence for privacy purposes. We are interested in the situation where the sequence to be scrambled is bandlimited and it is desired that the scrambling operation not expand the bandwidth. We will show how to find linear orthogonal invertible scrambling transformations which result in a negligible expansion of bandwidth. In Part II of this paper [3] we will apply these results to scrambling an analog waveform.

An outline of the paper is as follows. In Section I we review the definitions and properties of the spectrum (or Fourier transform) of a sequence and discuss the notion of bandlimited sequences. In Section II we formulate the scrambling problem and in Section III introduce discrete prolate spheroidal sequences which are an important tool in our solution of the scrambling problem. We discuss our scrambling scheme for deterministic and stochastic sequences in Sections IV and V. Section VI contains a generalization of our results to the bandpass case, and Section VII contains the proofs of the most involved theorems.

Abstract—The techniques developed in Part II [1] for discrete-time analog scrambling are applied to the problem of scrambling band-limited continuous-time signals or waveforms. The idea behind the waveform scrambler is to sample the waveform (which is assumed to be band-limited) at a rate exceeding the Nyquist rate. The resulting sequence of samples is band-limited in the sense of Part I. The discrete-time scrambler described in Part I is applied to this sequence to produce a nearly band-limited scrambled sequence. A scrambled waveform is formed by modulating the amplitudes of a chain of pulses. This scrambled waveform can be transmitted over a band-limited channel, and the original unscrambled waveform can be recovered at the receiver.

I. INTRODUCTION

IN THIS PAPER we apply the techniques developed in Part I [1] for discrete-time analog scrambling to the problem of scrambling band-limited continuous-time signals or waveforms for privacy purposes. The essential idea behind the waveform scrambler is to sample the waveform (which is assumed to be band-limited) at a rate exceeding the Nyquist rate. The resulting sequence of samples is a band-limited sequence in the sense of Part I. We then apply the discrete-time scrambler described there to this sequence to produce a nearly band-limited sequence. We next form a scrambled waveform by modulating the amplitudes of a chain of pulses with the scrambled sequence (PAM). We shall show that this scrambled waveform can be transmitted over a band-limited channel and that the original unscrambled waveform can be recovered by a receiver possessing the "key" to the scrambling operation. We treat two forms of the system: a basic version in Section II, and a complete version in Section III. Section IV is devoted to proofs of the theorems stated in Sections II and III.

Appeared in IEEE Trans. on Information Theory, VOL.IT-25, No 4 July 1979