RECENT DEVELOPMENTS IN NARROWBAND ANALOG SIGNAL ENCRYPTION WITH EMPHASIS ON VOICE CHANNEL SYSTEMS

Sergei Udalov
Axiomatix
Los Angeles, California 90045

ABSTRACT

In many instances, the process of telemetering of scientific information must be accompanied by a voice conversation which either reveals the sequence of measurements or provides information as to the nature of the data gathered and/or transmitted. If such voice information can compromise the integrity of the telemetry data to an unauthorized interceptor, voice privacy equipment must be used along with the equipment used for transmission of the telemetry data.

The recent developments in LSI technology provide a new capability to the design of voice encryption equipment. This is particularly true for the case where sophisticated analog encryption schemes must be employed to permit the encrypted voice information to be transmitted over the existing telephone and radio channels which are typically limited to a 3 KHz upper-frequency cutoff.

This paper examines the recent developments in analog voice privacy equipment design, as indicated by the disclosures made in open literature by various manufacturers and evaluators of such equipment. Advances in the technology as well as in analytical definitions of analog voice privacy are discussed. The role of such valuable LSI chips as a microprocessor and the DES algorithm are examined. Also, in addition to considering the classic frequency/time domain permutation algorithms, developments in analog "pseudonoise" scrambling are examined in view of the data made recently available in open literature.