DIGITAL TRANSMISSION OF VOICE

A study for the
Department of Communications
Ottawa, Ontario, Canada

by

Dr. Peter O. Brackett
Associate Professor
Department of Electrical Engineering
Queen's University
Kingston, Ontario

March 1978

DIGITAL TRANSMISSION OF VOICE

A study for the
Department of Communications
Ottawa, Ontario, Canada

by

Dr. Peter O. Brackett
Associate Professor
Department of Electrical Engineering
Queen's University
Kingston, Ontario

March 1978

ABSTRACT

The problem being considered in this study concerns the difficulty of observing and monitoring the telecommunications traffic flowing through an interconnection between a digital network and the public switched network. The purposes of monitoring are to determine which of the many possible such circuits carrying this traffic are being used for digital voice and to obtain irrefutable evidence of such use.

The state-of-the-art of voice digitizing and data encryption technology is reviewed with the conclusion that it is quite feasible to use such an interconnection for the purposes of digital voice communication. Digital secure voice terminals required for implementing this usage are now available for costs in the range of $15,000 to $35,000 depending upon the voice quality and security levels desired. Costs for similar terminals in the period 1980-1985 are projected to be in the range of $750 if user demand warrants the production of LSI devices.

A pragmatic method of estimating the cost of a monitoring system suggests that in the absence of secure channels it would require a capital outlay of approximately $2,000,000 to monitor ten circuits at one interconnection centre. If data security (crypto) is used, it is suggested that no practical system is possible.

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

1.1 The Problem Statement

The central problem to be investigated by this study may be described as follows. Suppose that two communications networks are interconnected; one being the public switched telephone network, and the other being either (i) a packet switched data network, or (ii) a circuit switched data network. Each of these networks carry "digital" signals, some of which are "data signals" i.e. they are machine generated and are intended for communication with other machines. Other digital signals may be carrying encoded voice primarily for the purpose of interpersonal communication. The digital voice encoding may be accomplished using vocoders, codecs, etc. In perhaps an extreme scenario, the encoded digital voice may be scrambled or enciphered by an encryption device, the enciphering algorithm and key of this device being known only to the network user and unknown to the network carriers.

The scenario depicted above is illustrated in Fig. 1.1. Given the interconnection and signals as described, the problem is to evaluate the technical feasibility and practicality of monitoring at the interconnection points, in particular at the analog circuit pairs of the public switched network, the circuits to determine and identify with reasonable certainty those circuits which are being used for voice communications. Such an identification should provide an unambiguous indication, suitable for

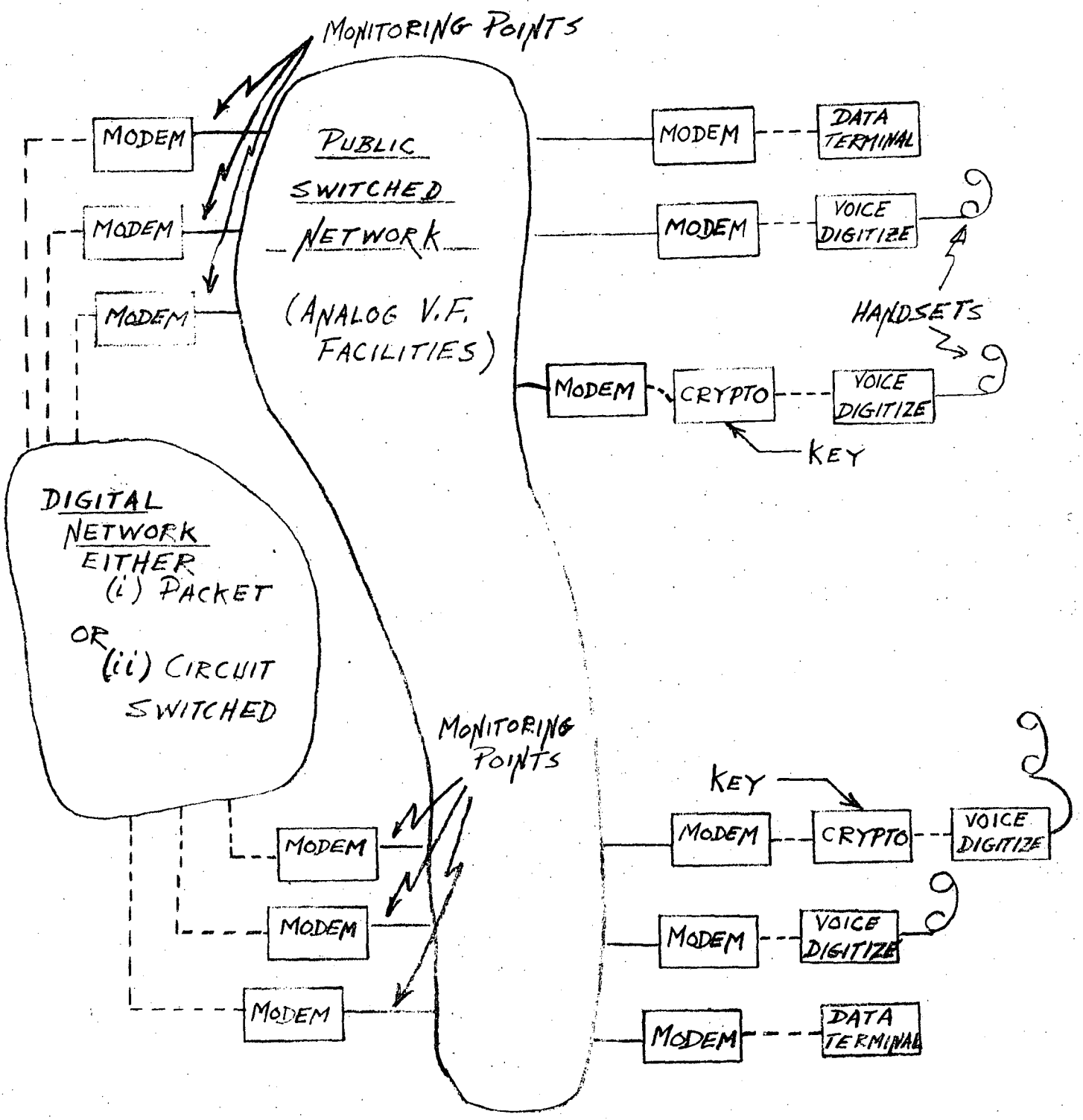


FIG. 1.1

THE SCENARIO

legal purposes of determining if the interconnection is carrying interpersonal (voice) traffic or intermachine (data) traffic.

Further, if possible, the capital and operating costs, including an indication of the type of technology required, for implementing any practical system to carry out this monitoring service is to be estimated.

1.2 Other Objectives of the Study

The main objective of the study is described in the last two paragraphs of Section 1.1, however as background, it is necessary to review the technology and costs for both voice digitizing and encryption equipment.

Thus, a further objective of the study is to conduct a survey of the state-of-the-art development and costs of voice digitizing equipment including vocoders, codecs, etc., as applied to voice communication in both a packet switched and a circuit switched digital data network environment. The quality of performance of these devices in terms of intelligibility, articulation index, fidelity and naturalness of voice for various types and bit rates will be reviewed, and the relative suitability of the two types of switched digital networks for full duplex voice communication using digitized voice will be examined.

Another objective of the study is to conduct a state-

of-the-art survey, including costs, of commercially available devices for encryption suitable for use with voice digitizing equipment.

A final objective is to forecast the costs of both voice digitizing and encryption equipment for the period 1980-1985.

1.3 Outline and Summary of the Study

The study is organized in an order reverse to that described in the previous sections since it is both more efficient and pedagogically convenient to present this material in a constructive rather than analytical manner. Thus the extreme scenario described in section 1.1 will be treated after the development of background material on digitization encryption and networks.

The outline of the study is as follows. Section 2 reviews the state-of-the-art and technology of voice digitizing equipment which provides the setting for the digital nature of the signals that are the subject of the proposed monitoring equipment.

Section 3 reviews the state-of-the-art and technology of data encryption equipment suitable for enciphering the digitized voice signals.

In Section 4, the scenario of Fig. 1.1 is reviewed in the light of Sections 2 and 3 together with additional

information on the characteristics of data MODEMs and the characteristics of digital voice in both the packet and circuit switched environments.

Finally, in Section 5, the central problem of monitoring and identifying digitized voice circuits is attacked.

Section 6 concludes with a summary of results, conclusions, suggestions and recommendations.

Section 7 presents the summarized and indexed results of a patent search undertaken to aid in the determination of the present state-of-the-art of the subject areas discussed in the study.

2 VOICE DIGITIZING EQUIPMENT

2.1 Introduction

Schemes for digitizing speech may be broadly classified into two groups, namely those schemes which model the human vocal apparatus with appropriate analysis and synthesis techniques and subsequently digitize and transmit parameters extracted from the model and those schemes which use direct digital encoding of the voice signals with perhaps additional "tricks" used for reducing the resultant data rate.

The oldest example of the first group is the so-called "channel vocoder" invented in the 1930's [1,2]. The term vocoder is a shortening of the two words VOice and CODER. The earliest and simplest example of the second group is known as PCM or Pulse Code Modulation [3,4]. Two excellent references on this subject in terms of their tutorial, historical and bibliographic completeness are the review of vocoders by Schroeder in 1966 [5] and the very recent review of digital voice by Gold in 1977 [6]. Those readers interested in a complete review and tutorial on voice digitization are referred to the above papers, and the additional references listed at the end of this section.

For purposes of this study, due to the nature of the problem being addressed, only a subclass of the various types of voice digitizers are of interest. Namely those

types which can produce "acceptable" voice transmission at bit rates up to 9600 bps. This restriction is caused by the fact (see Fig. 1.1) that signals on the circuits being used must pass over the public switched telephone network. Presently (1978), "reliable" data transmission on this network is restricted to 9600 bps and lower.

However, since comparisons both quantitative and subjective are often drawn between "telephone quality" PCM and other methods, a short digression to consider PCM is in order. The fundamental concepts involved in PCM are illustrated in Fig. 2.1. First, the speech signal is passed through an "anti-aliasing filter to eliminate any spectral components above a certain frequency f_c. The resulting speech is then sampled at a frequency f_s, which must be greater than the "Nyquist frequency" $2f_c$. The resulting samples are then quantized in amplitude by an Analog to Digital (A/D) converter which converts the samples to a binary code of b bits per sample. The quantization may be uniform or non-uniform. The bit stream (or bus) leaving the A/D converter is the digitized voice. The digitized voice may now be transmitted over a "digital" network.

The process of reconstructing the voice at the receiving end is also illustrated in Fig. 2.1. Here, the digitized voice is converted by a b bit Digital to Analog (D/A) converter to analog samples and passed through

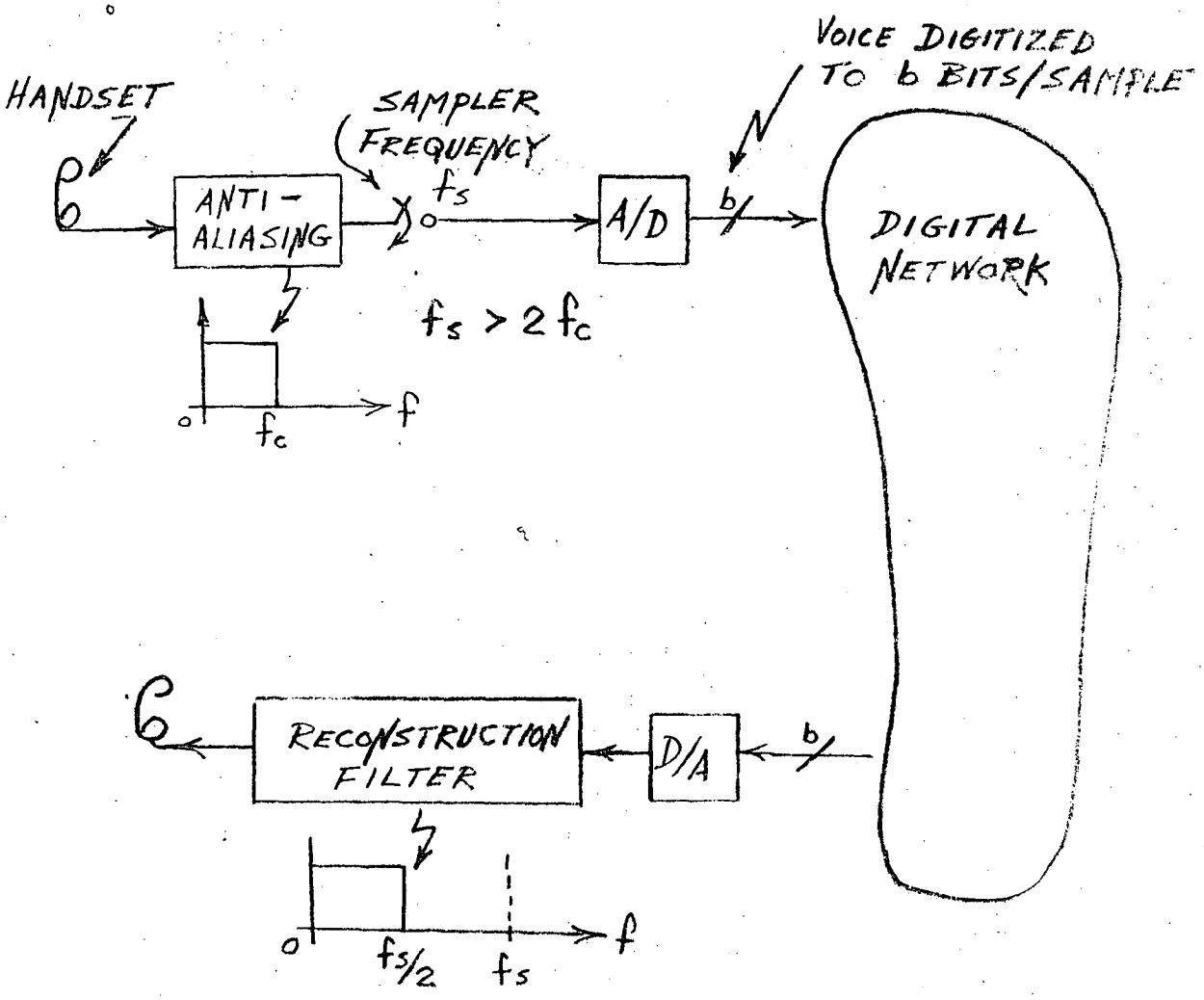


FIG. 2.1

FUNDAMENTAL CONCEPTS OF PCM

a "reconstruction" filter of bandwidth $\frac{1}{2}f_s$. The resulting waveform is a close facsimile of the original speech. Clearly, the larger the values of f_c, f_s and b, the more faithful is the replica produced at the receiver.

Engineering economics dictates that f_c, f_s and b should be as small as possible consistent with maintaining some minimum level of a performance measure. A well known standard used in conventional telephony has $f_c \simeq 3.5$ kHz, $f_s = 8$ kHz and $b = 8$. A heuristic justification of these numbers runs as follows. Telephone circuits have a "nominal" bandwidth of 3 kHz, and $f_s = 8$ kHz leaves some guard band for aliasing error. The signal to noise ratio (SNR) of telephone circuits is nominally 30 dB. Noting that $20 \log(2^b) \simeq 6b$, it seems that $30 \div 6 = 5$ bits suffices to represent the smallest detectable signal relative to the average signal level. Since the "typical" peak to average ratio of speech is near 14 dB, an additional 3 bits is required to allow for the total dynamic range from noise level to voice peaks, thus $b = 8$.

This set of numbers yields the serial bit rate of 8 kHz × 8 bits = 64 kbs found in typical PCM telephony equipment. Telephone users universally agree that the quality of the received speech is easily comparable to that of non-PCM telephone circuits.

A point to note here is that many users, in particular prospective users of the voice circuits in the scenario of

Fig. 1.1, can easily tolerate a much worse quality than that described here as "telephone quality". Professional communicators, such as, armed service personnel, taxicab drivers and the like are accustomed to voice communications over circuits with $f_c \simeq 2$ kHz and SNR = 12 dB, resulting in $f_s = 4$ kHz and b = (12 ÷ 6) + 3 = 5 bits which yields a serial bit rate of 4 kHz × 5 bits = 20 kbs, a factor of 3.2 less than telephony PCM.

The following sections review the state-of-the-art of voice digitizing equipment which produce data streams at less than 9600 bps, however, the point noted above is applicable to most digitizing schemes and when lower quality voice can be tolerated, simpler and more economical schemes can be applied.

PCM as described above does not take into account the statistical properties of speech. At a "normal" speaking rate of 300 words per minute, an average length of 4.5 characters per word and an average entropy of 2.3 bits per character, the information rate of speech is approximately 60 bps. In fact, if additional redundancy due to the statistical dependence between words, sentences, etc. is included, the actual rate is even less. The figures entering the above calculations have been obtained from a paper by Shannon [7] and others [8 , 9].

The above calculations show that it should be possible to design voice digitizing equipment which operates

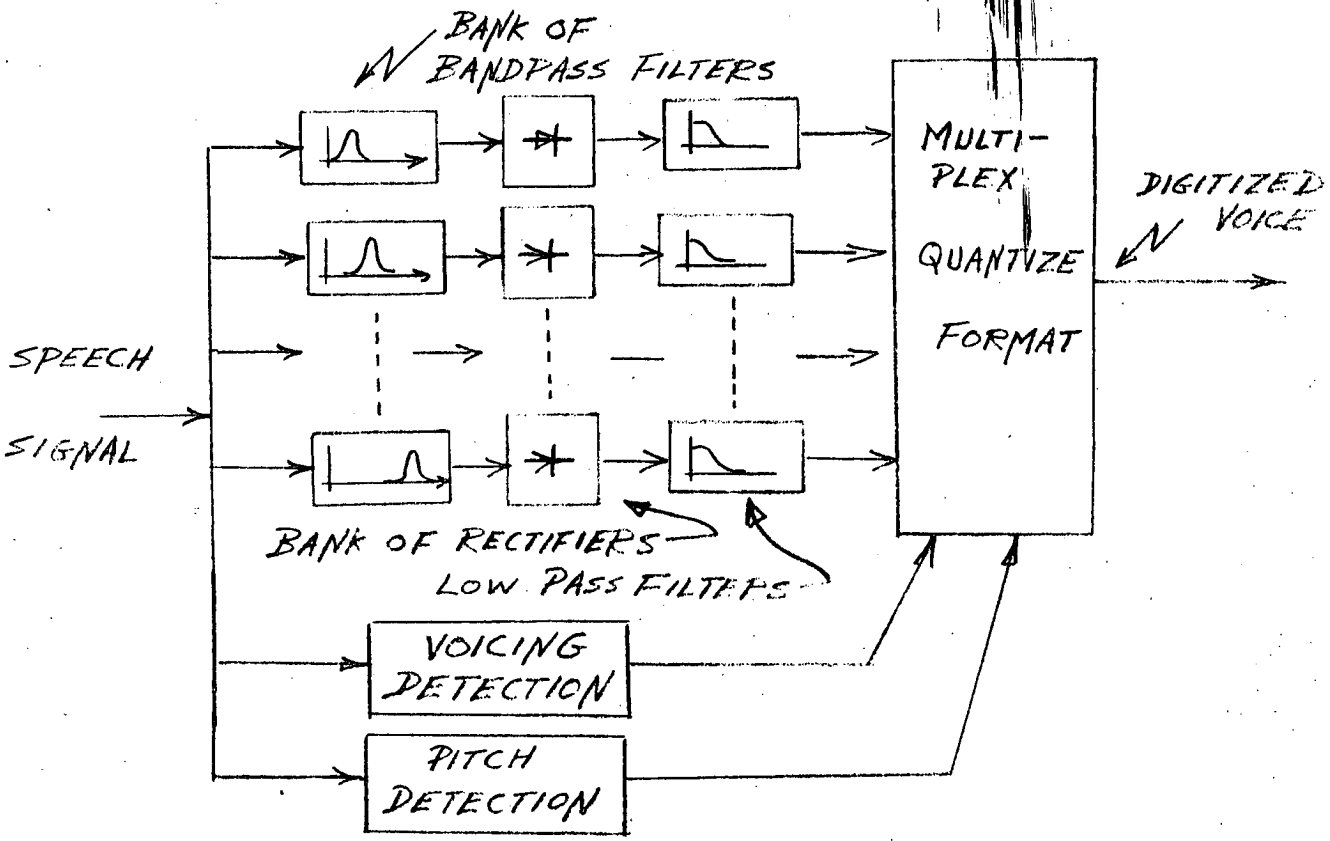
at a bit rate of less than 60 bps per voice channel. However, as with many of the results of Shannon's information theory, no synthesis methods for such systems are known. Instead, one can only propose systems within broad guidelines and compare the results with the theoretical limits. Invariably the cost of such equipment rises very quickly as the bit rate goes down towards the limiting rate.

Vocoders, and modified PCM systems do obtain lower bit rates than those described above for PCM systems. The systems to be described next, fall in the above class and have been found suitable for use at 9600 bps and lower.

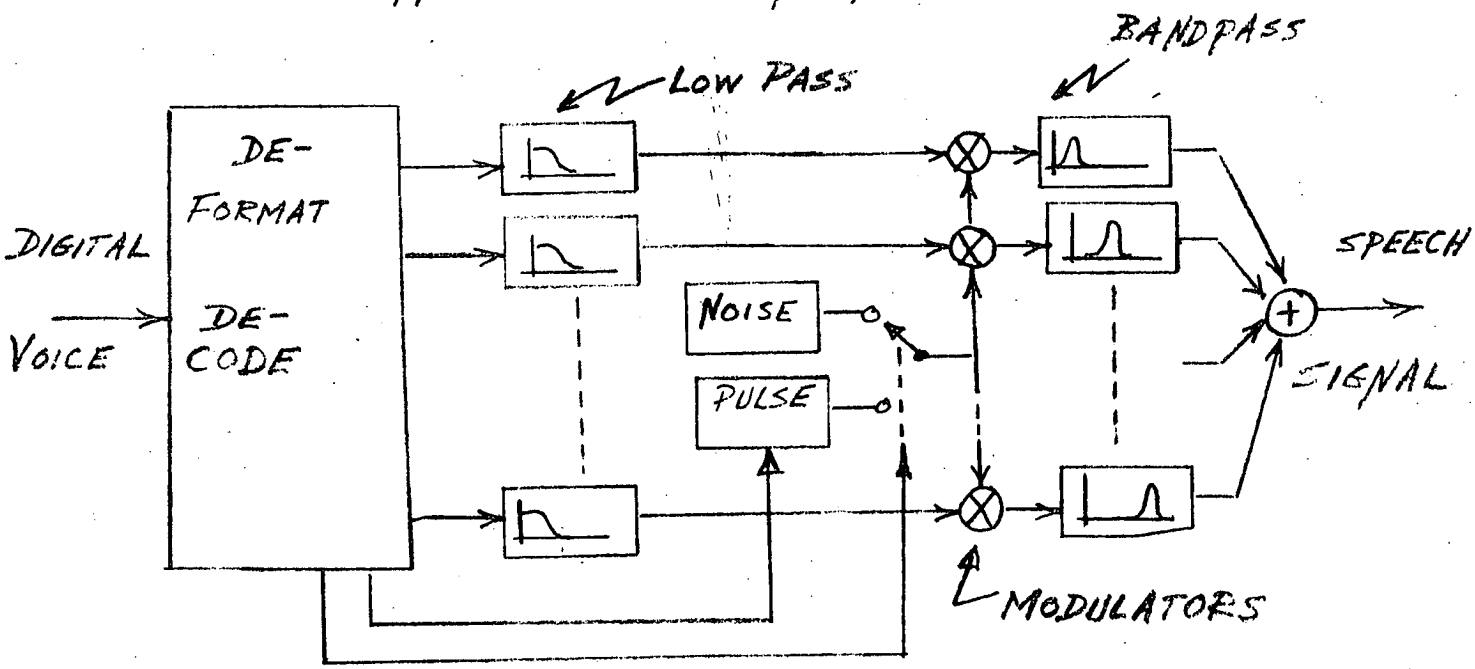
2.2 Voice Digitizers for Use at 9600 bps

2.2.1 Channel Vocoders

Fig. 2.2 is a block diagram of a channel vocoder which consists of an analyzer and a synthesizer. The analyzer accepts speech and produces a digital bit stream. The synthesizer accepts the bit stream and reproduces the speech. Note that the channel vocoder operates essentially as a spectrum analyzer making use of a bank of bandpass filters. As noted in [6], "We note that channel vocoders with significantly different design parameters have been experimentally shown to yield very intelligible speech. Despite nearly 40 years of research, no universal agreement



CHANNEL VOCODER ANALYZER



CHANNEL VOCODER SYNTHESIZER

FIG. 2.2

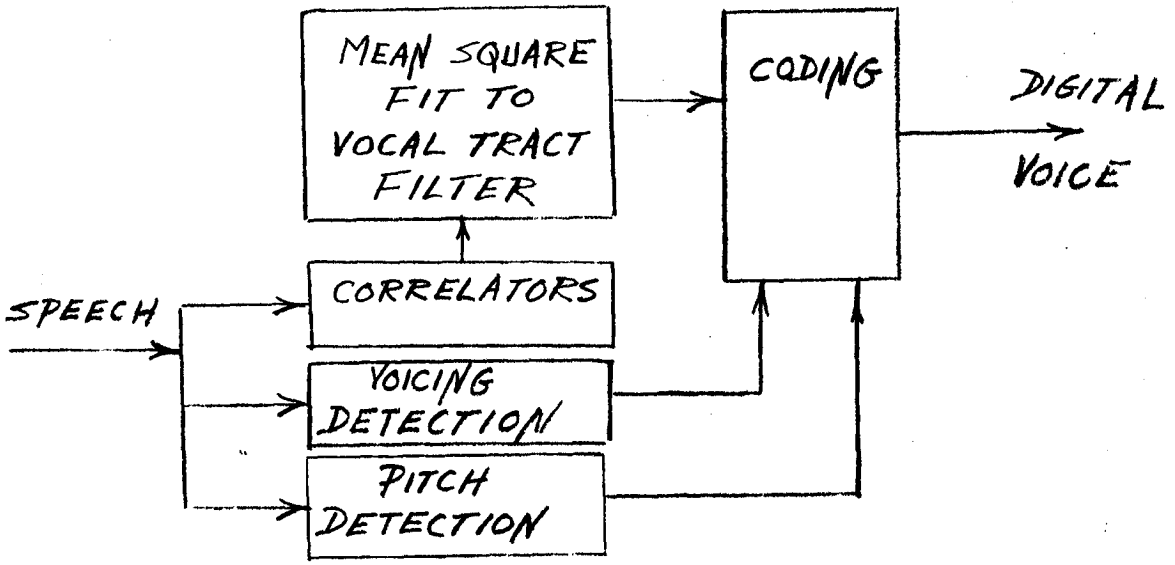
THE CHANNEL VOCODER

presently exists on the optimum design of channel vocoders for different data rates."

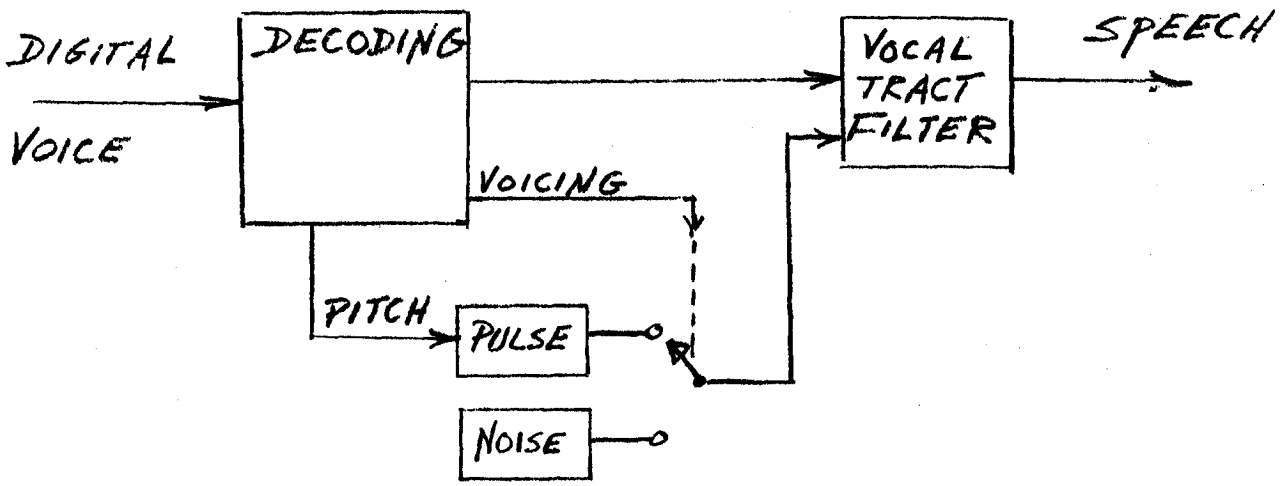
The channel vocoder was invented in the 1930's, but since the latter part of the 1960's, channel vocoder development essentially stopped, due to the advent of new and more economical devices. Telephone quality voice has been demonstrated at bit rates as low as 2400 bps. The original channel vocoders used analog filters, however, there may be a resurgence of interest in these devices with the advent of economical digital filter hardware.

2.2.2 Linear Predictive Coding (LPC) Vocoders

There has been a flurry of activity in the last five years in the area of LPC vocoders [10,11,12,13]. Fig. 2.3 is a block diagram of an LPC vocoder. The principle of the LPC vocoder is that a reasonable prediction of a sample of a speech wave can be based on a linear weighted sum of previous samples. Hence, the terms linear and predictive. The performance of LPC vocoders vis-a-vis channel vocoders operating at the same bit rate has yet to be established. The promising aspect from the viewpoint of this study is that LPC vocoders may be less expensive to implement. Although, with the emergence of inexpensive digital filtering hardware, this advantage could easily disappear.



LPC VOCODER ANALYZER



LPC VOCODER SYNTHESIZER

FIG. 2.3

LPC (LINEAR PREDICTIVE CODING) VOCODER

2.2.3 Homomorphic Vocoder

With the advent of the Fast Fourier Transform algorithm (FFT) and the emergence of inexpensive and fast digital filtering hardware, a new algorithm for vocoding called the "homomorphic vocoder" has appeared [14,15]. The block diagram of a homomorphic vocoder is shown in Fig. 2.4. The principle of the homomorphic vocoder is based on the fact that voice can be modelled as the convolution of an excitation function with the vocal tract filtering function. Taking the Fourier transform of a short speech segment or frame then obtains a spectrum which is the product of the transforms of the two functions. Taking logarithms of the spectrum then results in a sum of two functions. One of these is rapidly varying (excitation) and the other is slowly varying (vocal tract). These variations are, of course, in the spectral domain. Thus, these two components in the sum may be separated by filtering. This filtering is performed by a further Fourier transform. The two resulting functions are then encoded for reduced rate data transmission on a frame by frame basis. The inverse or synthesis operation involves computing the impulse response of the vocal tract and convolution of it with the excitation function, an operation that is again facilitated by the FFT algorithm, and also involves an exponentiation.

The computational effort required to perform the homomorphic algorithm is large, but well within the

FFT ~ FAST FOURIER TRANSFORM

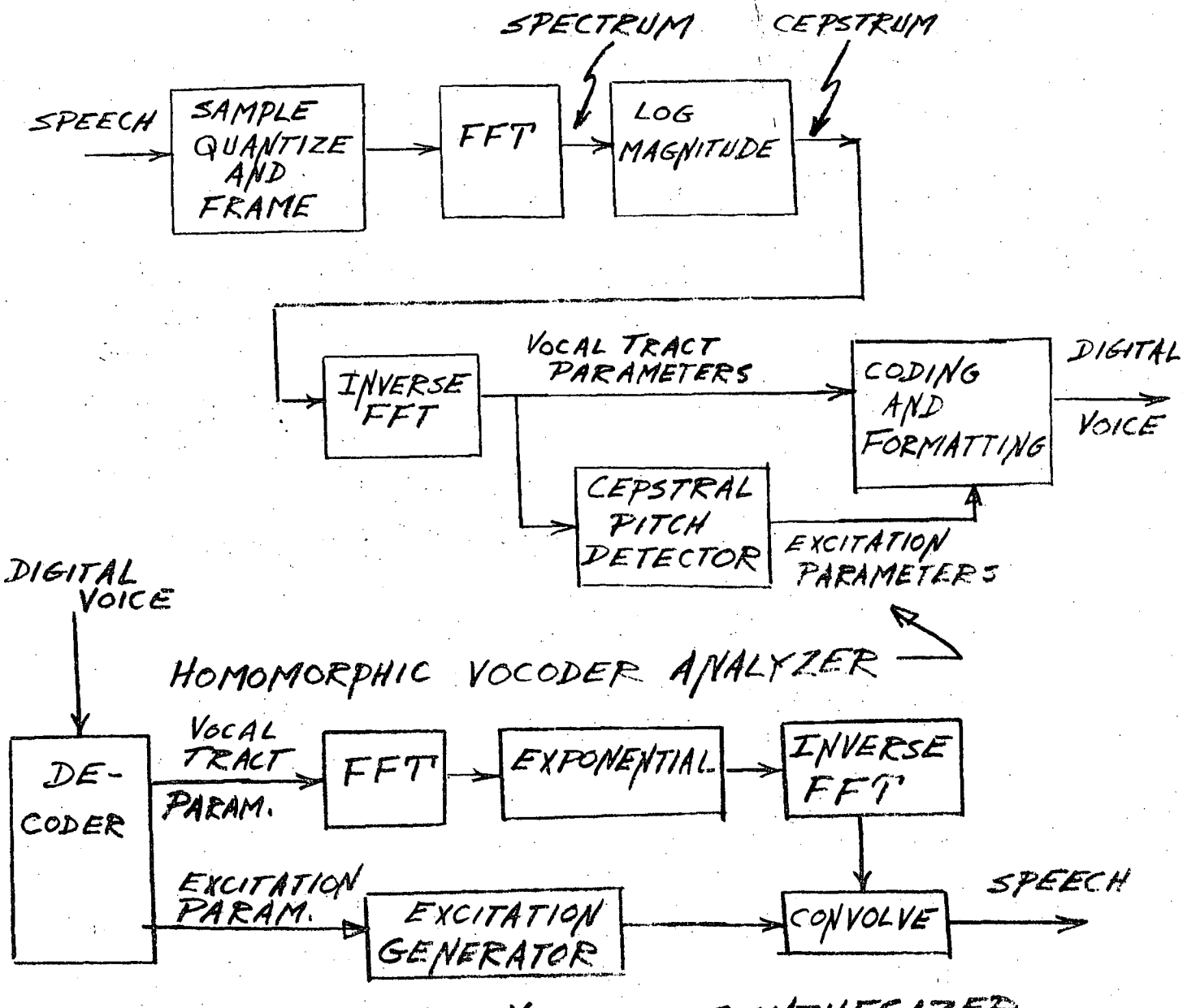


FIG. 2.4

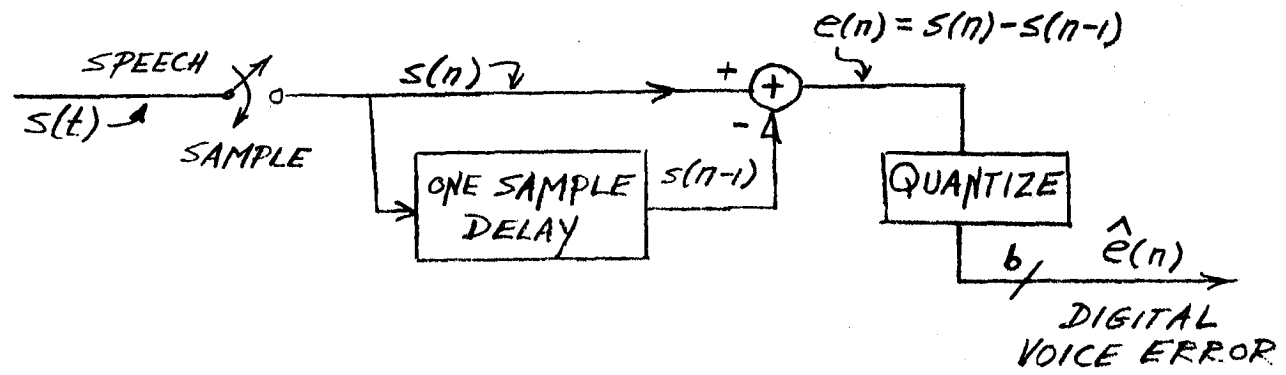
THE HOMOMORPHIC VOCODER

processing capabilities of modern digital signal processing hardware. It tends to be expensive.

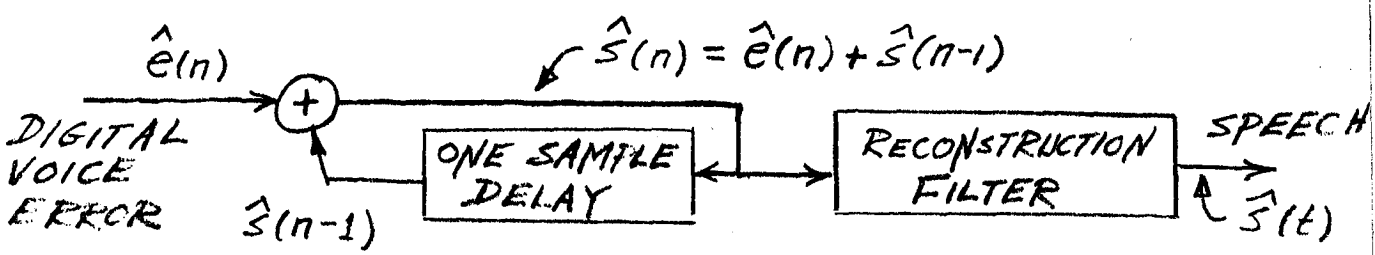
2.2.4 Delta Modulation Code-Decoding (CODECs)

A group of speech encoding algorithms based on the premise that fewer bits are required to encode the derivative of speech than the speech itself give rise to a number of differential PCM or delta modulator (DM) techniques. These are generally termed predictive methods. Fig. 2.5 illustrates the simplest form of DM. Note that the difference between successive speech samples is encoded. A simple DM circuit for A/D conversion is given in [16]. Many references on DM can be found in [17]. Simple, direct DM as shown here is not suitable for voice transmission at 9600 bps, however, several modifications of DM do show promise.

One of these methods termed Adaptive Differential PCM (ADPCM) is illustrated in Fig. 2.6. Here, the quantizer of Fig. 2.5 is made adaptive by controlling it with the volume of the incoming speech. The volume signal V performs the function of compressing and expanding the adaptive quantizer in accordance with the volume which varies at a syllabic rate. Note that the volume information must be formatted in frames with the variable length DM data. Both DM and ADPCM are susceptible to a phenomenon termed slope overload distortion. This is a "slewing" problem caused by the fact that the CODEC cannot slew fast enough



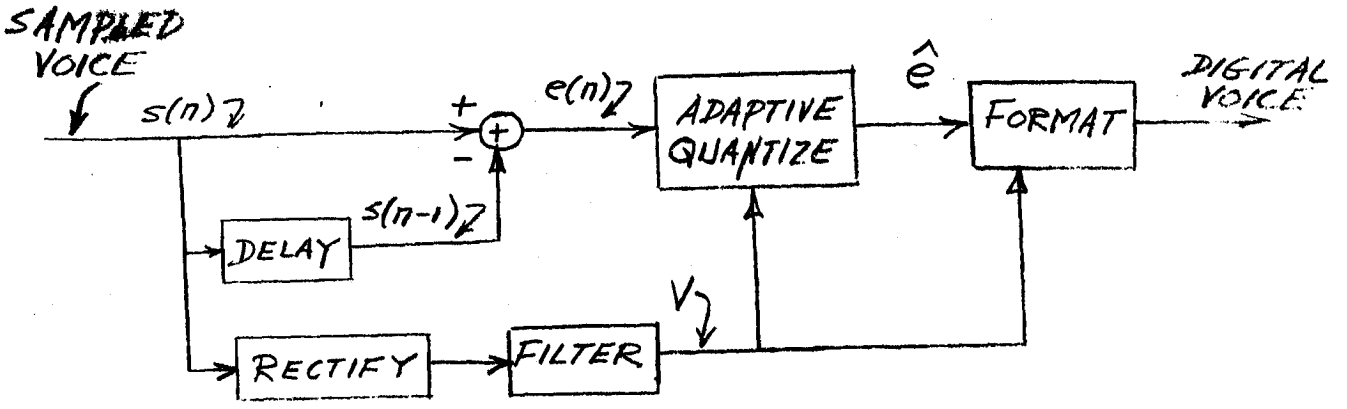
DIFFERENTIAL PCM MODULATOR
(DELTA MODULATOR)



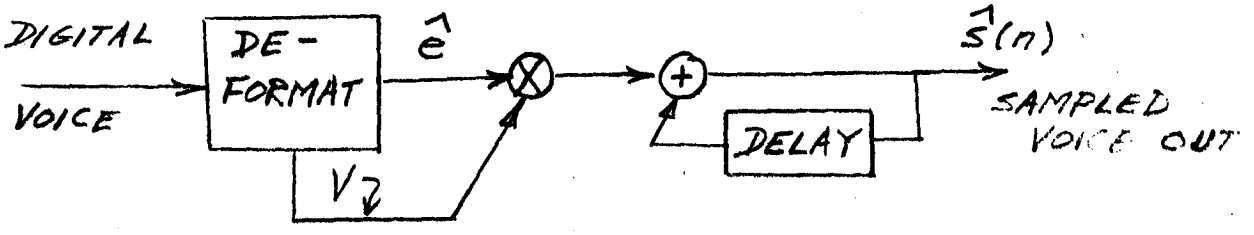
DIFFERENTIAL PCM DEMODULATOR

FIG. 2.5

A SIMPLE DELTA MODULATOR CODEC



ADPCM MODULATOR



ADPCM DEMODULATOR

FIG. 2.6

ADAPTIVE DIFFERENTIAL PCM CODEC.

to follow fast rising or falling waveforms.

A further refinement termed Continuously Variable Slope DM or CVSD is often used. In this CODEC, the slope of the signal is sensed and used to control the quantizer resulting in less slope overload distortion [18].

2.2.5 Adaptive Predictive Vocoder (APC)

The predictive ideas from the DM techniques can be combined with the LPC vocoder to produce an Adaptive Predictive Coder (APC). This relatively new concept has been extensively tested [19]. In this system, prediction is based both on the measured value of the speech one period back which produces an error or differential code, and an LPC coding of this first error signal. The fundamental period is measured by a pitch detection algorithm. The differential error signal transmitted is computed by a feedback loop using adaptive parameters.

2.3 Relative Performance Characteristics

The channel vocoder, LPC vocoder and homomorphic vocoder of sections 2.2.1 through 2.2.3 utilize some form of modelling of the human voice process and achieve the lowest bit rates for "good" quality voice. These devices provide "good" quality voice at bit rates in the

range of 2400 to 9600 bps. However, it should be pointed out that such systems are not as "robust" as the predictive techniques.

The quality of robustness refers to the sensitivity of the devices to bit errors in the data stream, and background acoustic noise. Such a result is not unexpected since much of the redundancy in the voice has been removed, thus providing a lower level of the inherent error protection contained in wideband speech.

The predictive techniques based on delta modulation such as the DM, ADPCM, and CVSD CODECs must operate at rates above about 16 kbs to produce "good" quality speech. These devices, as expected, are much more robust than the vocoding methods based on voice modelling described above. However, DM CODECs are much more economical than vocoders. These devices can provide "communications" quality voice at rates as low as 4800 bps. Some of these devices are quite remarkable in their performance at 9600 bps. This author has personally used a system with a DM CODEC, 9600 bps CCITT V.29 MODEM and a telephone handset over the public switched telephone network, and found the voice quality to be far superior to that encountered in using HF SSB radio equipment.

The relatively new APC technique which combines modelling and prediction, thus representing a hybrid mix of the two types of digitizing equipment, shows promise

as the most cost effective method of producing "good" quality digitized speech at rates of 4800 to 9600 bps.

Both quantitative and qualitative evaluation of the various algorithms described here must be tentative since all of the algorithms are undergoing development and enhancement. Any evaluations must include the effects of data bit errors and background acoustic noise before the "practical" superiority of any particular method can be established.

The IEEE has published a standard [20] on voice quality measurements, and at least one independent company namely,

Dynastat Corp.,
2704 Rio Grande,
Suite Four,
Austin Texas 78705
Tel. (512) 476-4797

provides comparisons and evaluations of various types of voice equipment. It should be noted that not all quantitative measurements are correlated with human preference, and good results on measurements such as signal to noise ratio, harmonic distortion and intermodulation distortion do not necessarily indicate that humans will prefer the voice reproduced by the "best" device in terms of these measurements. Thus, the "best" voice digitizing equipment can only be judged by subjective testing using critical human recievers.

A number of papers [21,22] give the results of subjective evaluations of several of the predictive techniques to which the reader is referred for details.

To this author's knowledge, no one has performed an objective (double blind) series of subjective tests to compare all of the voice digitizing algorithms. Thus, the comments on "good" and "communications" quality voice together with the individual authors or inventors evaluations of their own techniques, which may be found in the references, are left with the reader as a basis for making his own judgements. It suffices to say that a number of techniques exist, having various degrees of cost effectiveness, which are quite suitable for application to the scenario of Fig. 1.1.

2.4 Commercial Products, Costs and Summary

In relation to the predictive devices, vocoders are generally more expensive to implement due to their additional complexity. This cost may become inconsequential with the advent of economical LSI digital signal processing hardware. If the sales volume warrants production of LSI vocoders, their price could become competitive with the generally more economical predictive techniques. It should be noted that LSI high speed (9600 bps) data MODEMs are now available, and the computational complexity of these devices is comparable to that of vocoders. Appli-

cation of the same technology to vocoders should result in much lower prices than those quoted later in this section.

Since the DM based CODECs are simpler than vocoders, they are, of course, more economical, and are presently being implemented and sold in IC form [23,24]. At the present time, in the scenario of Fig. 1.1, this author feels that the most cost effective solution for voice digitization is the accaptance of "communications" quality voice and the use of one of the commercially available DM CODECs at 9600 bps. Of course, this service would not be suitable for offering to the general public.

Just in the past year, this author has spoken on and used a digitized voice system consisting of a handset, DM CODEC, and 9600 bps MODEM operating over the switched telephone network. The cost of the CODEC (non LSI) was $1500, and the MODEM (non LSI) $8500, for a total cost of about $10k. The MODEM was the new 96Qm CCITT V.29 MODEM introduced by ESE Limited, when this author was employed there as Chief Development engineer. The two devices could easily have been incorporated into the same chassis.

E-SYSTEMS INC. produce a commercial digital speech processor called the VADAC 5. This device can produce a digitized voice and multiplex in a low speed data channel simultaneously. It is a homomorphic vocoder and runs at data rates of 2400 bps or 4800 bps. They

claim that operation at bit error rates in the neighbourhood of 2 in 10^3 or less yields essentially the same operation as zero error rate. It is outfitted with standard digital interfaces (CCITT V.24 and RS232). A built in MODEM (Bell 201 card MODEM) can be fitted as an option. The size is 7" x 19" x 18", weight 45 lbs. A telephone quoted price (Feb. 1978) was $13,985 US in quantities of 10 or less without MODEM. The price drops to $11,343 US for quantities of 100 or more. Descriptive literature is available from the company at the address listed in the references. This company also manufactures a complete secure voice terminal which will be described in section 3.

TIME AND SPACE PROCESSING INC produce a commercial LPC vocoder called the Model 100. This device operates at 2400/4800 bps and also can multiplex in a low speed data channel. This device has been given a rating of 92 by DYNASTAT, the evaluation company mentioned in section 2.3. On a similar scale the common carbon microphone used alone produces voice quality rated at 95. The Model 100 has standard (CCITT V.24, RS232, and MILL 188) digital interfaces. The price of this vocoder in unit quantities from a telephone quotation (Feb. 1978) was $15,250 US, with quantity discounts for 8 or more units of $11,250. Note that it is very competitive with E-SYSTEMS' VADAC 5. Again descriptive literature is available from the company at

the address listed in the references. People at other companies dealing exclusively with encryption equipment, stated to this author that the Model 100 was the "best" vocoder on the commercial market.

A number of other companies produce vocoders both commercially and for military secure voice use. Some of these are listed in the references.

Clearly, at the quoted prices, the use of vocoders will not become widespread. Note however that the costs quoted are only about twice that of a 9600 bps data MODEM suitable for public switched network use. If vocoders were produced in the same volume as MODEMS, their costs today would be comparable.

A number of non-commercial laboratory type vocoders, both special and general purpose, have been described in the literature [25,26,27]. It is possible to price some of these since almost complete parts lists are given in some references. Computations based on these lists including mark-up for labour and profit result in the same ballpark prices ≃ $12,000 as the commercial devices described above where the price is also controlled by competition. Thus, $12,000 represents a "fair" price for a high quality 4800 bps vocoder in today's market (1978). Gold [6] in an article of Data Channels [28] states that he expects vocoder prices to reach ≃ $500 in 5 to 7 years. This is, of course, possible using LSI technology, but will

only happen if volume sales warrant it.

SED SYSTEMS LTD. in Canada produce a Model 6090 DELTA CODEC which they recommend for use at rates between 19.2 kbps and 40 kbps for "good" quality. However, as mentioned earlier, this author has used it at 9600 bps and found acceptable "communications" quality voice. This CODEC mounts on one plug-in board and sells for ≃ $1500 CAN. Another Model 5540 utilizing thick film technology has similar performance and sells for ≃ $800 CAN. These devices could very easily be integrated and probably sold in volume for prices under $50 CAN. Presently, a number of IC manufacturers are producing or developing IC CODECs and there seems to be a lot of activity in this area [23,24].

In summary, there are a number of choices of voice digitizing equipment available to users. These devices have different prices and performance. Generally price and performance are directly related. Thus, a user can select the "best" device for a cost effective solution to his particular voice digitizing requirements. The costs of presently available equipment have been indicated, and cost projections for the next 5 to 10 years have been provided. The following section contains a number of references for the material of this section.

2.5 References

The following references include in numerical order, those quoted in the text, followed by other references of general or special interest in the field of voice digitization. A list of U.S. patents of specific interest selected from the cross-indexed list of section 7 is also given. Finally, a list of companies selling voice digitizing equipment is given together with the names of those company representatives who supplied the telephone quotations in this section.

[1] H. Dudley, "Remaking speech," J. Acoust. Soc. Am., Vol. 11, pp. 169-177, 1939.

[2] B. Gold and C.M. Roder, "The channel vocoder," IEEE Trans., Vol. AU-15, pp. 148-160, Dec. 1967.

[3] H.S. Black, "Modulation Theory," D. Van Nostrand, Princeton, N.J., 1953.

[4] H.S. Black, et. al., "Pulse code modulation communication system," U.S. Pat. No. 3,020,350., Feb. 6, 1962.

[5] M.R. Schroeder, "Vocoders: analysis and synthesis of speech (a review of 30 years of applied speech research)," Proc. IEEE, Vol. 54, No. 5, pp. 720-734, May 1966.

[6] Bernard Gold, "Digital speech networks," Proc. IEEE, Vol. 65, No. 12, pp. 1636-1658, Dec. 1977.

[7] C.E. Shannon, "Prediction and entropy of printed English," BSTJ, Vol. 30, pp. 50-64, Jan. 1951. (Also appears in a collection of papers published by IEEE press. See, David Slepian, ed., "Key papers in the development of information theory, IEEE Press Selected Reprint Series, IEEE Press, 1973.

[8] H.E. White, "Printed English compression by dictionary encoding," Proc. IEEE, Vol. 55, No. 3, pp. 390-396, Mar. 1967.

[9] B.G. Taylor, "Entropy of delta coded speech," Proc. IEE, Vol. 123, No. 8, pp. 743-751, Aug. 1976.

[10] B. Atal and S.L. Hanauer, "Speech analysis and synthesis by linear prediction of the speech wave," J. Acoust. Soc. Am., Vol. 50, pp. 637-655, 1971.

[11] M.R. Sambur, "An efficient linear prediction vocoder," BSTJ, Vol. 54, No. 10, pp. 1693-1724, Dec. 1975.

[12] J. Makhoul, "Linear prediction: a tutorial review," Proc. IEEE, Vol. 63, pp. 561-580, 1975.

[13] B.S. Atal, M.R. Schroeder, and V. Storer, " Voice-excited predictive coding system for low bit-rate transmission of speech," in Conf. Rec., Int. Conf. Commun., (ICC 75), San Francisco, CA., pp. (30-31) - (30-40), June 1975.

[14] A.V. Oppenheim, "Speech analysis-synthesis system based on homomorphic filtering," J. Acoust. Soc. Am., Vol. 45, pp. 459-462, 1969.

[15] L.R. Rabiner, "On the use of autocorrelation analysis for pitch detection," IEEE Trans., Vol. AU-25, No. 1, pp. 24-33, Feb. 1977.

[16] Leland B. Jackson, James F. Kaiser, and Henry S. McDonald, "An approach to the implementation of digital filters," IEEE Trans., Vol. AU-16, No. 3, pp. 413-421, Sept. 1968.

[17] S. Jayant, ed., Waveform quantization and coding, IEEE Press, New York, 1976.

[18] L.J. Greenstein, "Slope overload noise in linear delta modulators with Gaussian inputs," BSTJ, Vol. 52, pp. 387-422, Mar. 1973.

[19] B. Atal and M.R. Schroeder, "Adaptive predictive coding of speech signals," BSTJ, Vol. 49, No. 8, pp. 1973-1994, Oct. 1970.

[20] "IEEE recommended practice for speech quality measurements," IEEE Trans., Vol. AU-17, No. 3 pp. 225-246, Sept. 1969.

[21] R.W. Donaldson and R.J. Douville, "Analysis subjective evaluation and optimization of the performance capabilities of PCM, DPCM, DM, AM and PM voice communication systems," IEEE Trans., Vol. 4 COM-17, No. 4, pp. 421-431, Aug. 1969.

[22] J. Yan and R.W. Donaldson, "Subjective effect of channel transmission errors on PCM and DPCM voice communication systems," IEEE Trans., Vol. COM-20, No. 3, pp. 281-290, June 1972.

[23] Specification sheets for Motorola Devices MC3417/ MC3418 Voice encoding/decoding integrated circuits. Both types use the CVSD technique, the MC3417 is a 3 bit algorithm for military secure voice applications, and the MC3418 is a telephone quality 4 bit algorithm.

[24] See special session on CODECs (session 14) in the Proceedings of the International Solid State Circuits Conference, sponsored by IEEE in San Francisco, Feb. 1978.

[25] E.M. Hofstetter, Joseph Tierney and Omar Wheeler, "Microprocessor realization of a linear predictive vocoder," IEEE Trans., Vol. ASSP 25, No. 5, pp. 379-387, Oct. 1977.

[26] Shlomo Waser and Allen Peterson, "Real-time processing gains ground with fast digital multiplier", Electronics, Vol. 50, No. 20, pp. 93-99, Sept. 29, 1977.

[27] D.L. Cohn and J.L. Melsa, "The residual encoder - an improved ADPCM system for speech digitization", IEEE Trans., Vol. COM-23, No. 9, pp. 935-941, Sept. 1975.

[28] Data Channels, pp. 6-7, Jan. 1978.

[29] N.S. Jayant, "Digital coding of speech waveforms: PCM, DPCM and DM quantizers", Proc. IEEE, Vol. 62, No. 5, pp. 611-632, May 1974.

[30] S.C. Kak and N.S. Jayant, "On speech encryption using waveform scrambling", BSTJ, Vol. 56, No. 5, pp. 781-808, May - June 1977.

[31] R.E. Crochiere, "On the design of sub-band coders for low-bit-rate speech communication", BSTJ, Vol. 56, No. 5, pp. 747-770, May-June 1977.

[32] R.E. Crochiere and M.R. Sambur, "A variable band coding scheme for speech encoding at 4.8 kb/s", BSTJ, Vol. 56, No. 5, pp. 771-779, May-June 1977.

[33] Lawrence H. Goldstein and Bede Liu, "Quantization noise in ADPCM systems", IEEE Trans., Vol. COM-25, No. 2, pp. 227-238, Feb. 1977.

[34] Chong Kwan Un, and D. Thomas Magill, "The residual-excited linear prediction vocoder with transmission rate below 9.6 kbits/s", IEEE Trans., Vol. COM-23, No. 23, pp. 1466-1474, Dec. 1975.

[35] P. Noll, "A comparative study of various quantization schemes for speech encoding", BSTJ, Vol. 54, No. 9, pp. 1597-1614, Nov. 1975.

[36] P. Noll, "Effects of channel errors on the signal-to-noise performance of speech-encoding systems", BSTJ, Vol. 54, No. 9, pp. 1615-1636, Nov. 1975.

[37] M.R. Sambur, "An efficient linear-prediction vocoder", BSTJ, Vol. 54, No. 9, pp. 1693-1723, Nov. 1975.

U.S. Patents of Interest Selected from the Cross-Indexed Numerical List of Section 7

4,066,844; 4,070,709; 4,071,825; 4,074,069; 4,064,363; 4,061,878; 4,057,797; 4,001,505; 3,020,350; 3,071,649; 3,959,592.

LIST OF COMPANIES
SUPPLYING VOICE DIGITIZING EQUIPMENT

Controlonics Corp.,
1 Adams St.,
Littleton, MA. 01460
(617) 486-3571

Engineered Communications Inc.,
1610 Potomac Ave.,
Pittsburgh, PA. 15216
(412) 344-9000

E-Systems Inc.,
Garland Division,
P.O. Box 6118,
Dallas- TX. 75222
(214) 272-0515, Mr. Donald Fulghum

Kennedy Engineering Co.,
P.O. Box 2667,
Santa Fe Springs, CA. 90670
(213) 868-9965

Martin Marietta/Orlando Div.,
P.O. Box 583,
Orlando, FL. 32805
(305) 352-2087

SED Systems Ltd.,
P.O. Box 1464,
Saskatoon, Sask. S7K 3P7
(306) 244-0976, Mr. Andy Sendyk

Tele-Signal Corp.,
185 Oser Ave.,
Hauppauge, NY. 11787
(516) 273-3939

Time and Space Processing Inc.,
10430 North Tantau,
Cupertino, CA. 95014
(408) 996-2200, Mr. Charles Davis

3 VOICE ENCRYPTION EQUIPMENT

3.1 Introduction to Cryptography

Cryptography, the study of "hidden" messages, or secret codes and ciphers is almost as old as human written communication [1,2,3]. The lay reader will find a very entertaining historical and pseudo-technical account of cryptography in the references mentioned. Cryptography was originally applied only to written or "record" communications however, with the advent of modern electronics it has become possible to encript or encipher voice signals.

There are two separate methods of enciphering voice signals. The earliest method [4,5], which is still in use, operated directly on the analog (non-digitized) voice by performing spectral transformation. Examples of this type of voice "scrambler" are methods which "invert" the voice by modulation and demodulation such that the high frequencies in the voice become low frequencies and vice versa. Clearly, such a scheme is easily "unscrambled" by means of a simple modulation device. Variations of this technique involve splitting the voice spectrum into sub-bands and then permuting the bands. Modern devices provide digitally controlled time variable permutations. Commercial devices of this type are widely available and are reported in the patent literature [6, 7, 8]. Such systems, because they are relatively easy to unscramble, are usually termed voice "privacy" devices rather than

voice "encryption" devices or "secure" voice devices. These spectrum scrambling techniques are also being applied to television privacy systems for "pay TV" applications [4]. This type of voice encryption is not of interest in this study.

The second method of voice encryption applies standard data encryption techniques to a digitized voice data stream. This technique of first digitizing the voice and then encrypting the digits effectively separates the encryption and digitizing processes. Thus, if an encryption device or "crypto" unit is attached to a vocoder or CODEC, the result is a "secure" vocoder or CODEC. This combination is often termed a "secure digital voice terminal", and is illustrated in Fig. 3.1. Since the crypto device and the voice digitizing equipment may be viewed separately, it is useful to consider the crypto units separately.

There is a "jargon" associated with cryptography that is useful to know.

Plaintext - is the message that will be put in secret form.

Transposition cipher - the characters of the plaintext are shuffled, their normal order is disarranged.

Substitution cipher - the characters of the plaintext are replaced by other characters.

Cipher alphabet - is a list of equivalent characters used in substitution.

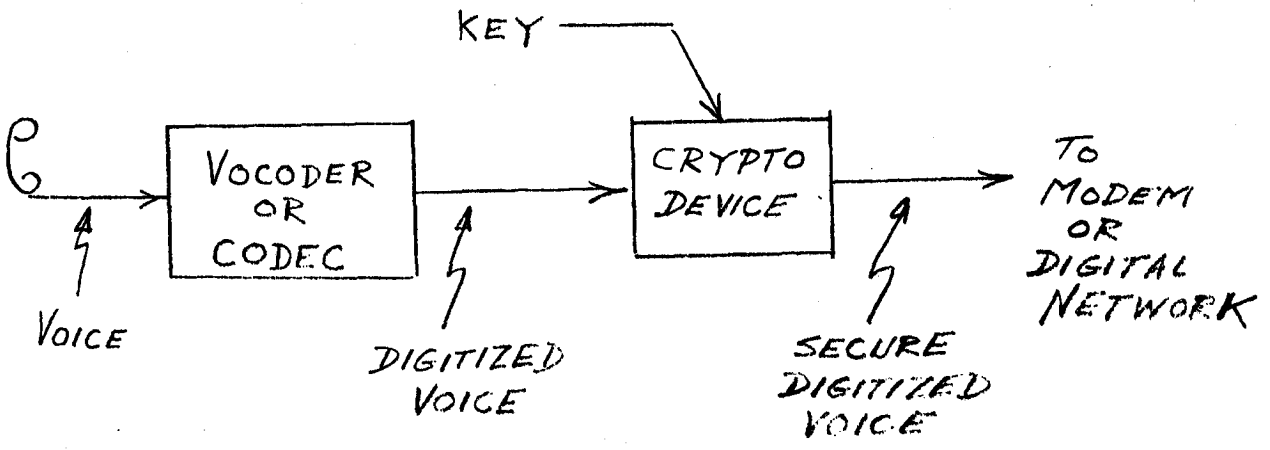


FIG. 3.1

A SECURE DIGITAL VOICE TERMINAL

Nulls - are characters or symbols which have no meaning and are inserted in the message to enhance confusion.

Monalphabetic substitution ciphers - use only one substitution cipher alphabet.

Polyalphabetic substitution ciphers - use many substitution cipher alphabets.

Key - a method of specifying the arrangement of characters in a substitution alphabet or the selection of cipher alphabets in a polyalphabetic substitution.

Encipher, Encode, Encrypt - the process of converting the plaintext to secret form.

Ciphertext - the secret text resulting from enciphering the plaintext.

Decipher, Decode, Decrypt - the procedure performed by a legal recipient of a ciphertext in recovering the original plaintext from the ciphertext.

Cryptanalysis, Codebreaking - the procedure performed by an "enemy", or person for whom a ciphertext is not intended, in recovering the plaintext.

Cleartext or *In Clear* - messages sent without being enciphered.

Unconditional Security - is provided by ciphers that can be proven mathematically to be immune to cryptanalysis.

Computational Security - is provided by ciphers for which it can be proven mathematically that the required cryptanalysis requires an algorithm of inordinate complexity in terms of an operation storage product.

Ciphertext only attack - is a cryptanalytic attack in which the cryptanalyst possesses only ciphertext.

Known plaintext attack - is a cryptanalytic attack in which the cryptanalyst possesses a substantial amount of plaintext and the corresponding ciphertext.

Chosen plaintext attack - is a cryptanalytic attack in which the cryptanalyst can (by perhaps devious means) submit his own chosen plaintext for encryption and examine the resulting ciphertext.

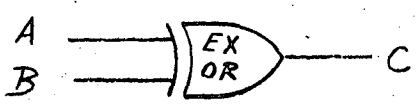
The history of cryptography runs back thousands of years. In this study, only those methods found useful with modern communications technology will be discussed. Further, it is almost certain that the military and secret service of certain government agencies have available knowledge and methods that are not available in the open literature. Consequently, there may be new and economical cryptographic systems which are classified and unknown to the general public. Such systems cannot be reported here. At the present time, public interest in cryptography is growing [9, 10, 11] due to the requirements of providing secure computer data banks and provision of authenticatable digital signatures for electronic funds transfer systems. In fact, in the past year, the U.S. National Bureau of Standards has introduced a standard for the cryptographic security of computer systems [12].

3.2 Classical Cryptography

In this section, well established systems of cryptography will be discussed. In a later section, some new directions in cryptography will be presented.

Until fairly recent times, cryptography has not had the benefit of a sound mathematical basis, and had been considered somewhat of a black art. The introduction of Information Theory by Claude E. Shannon [13] in his celebrated 1948 paper provided the basis for a mathematical treatment of cryptography. In fact, it was Shannon in 1949 [14] who wrote the first comprehensive mathematical treatment of cryptography and secrecy systems, and gave guidance for the design of good systems.

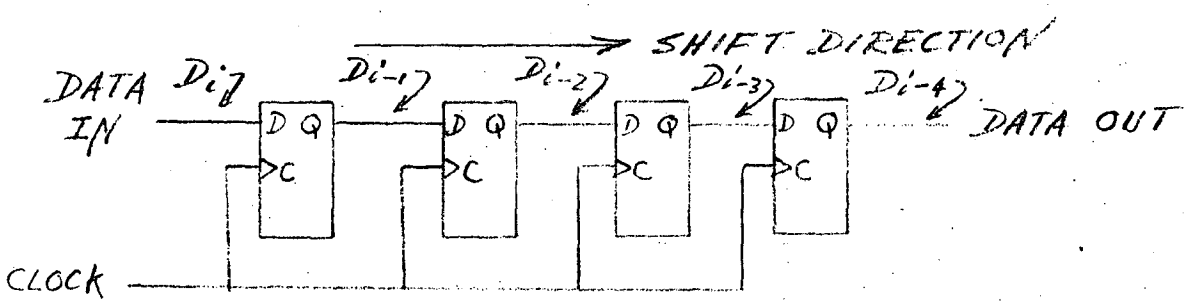
Most of the modern cryptographic systems are equivalent in operation to a system originally invented by Vernam [15,16,17,18]. This system can be put into a more modern easily understood setting by using digital logic diagrams. First, a logic function described variously as "exclusive or", ring sum, or modulo 2 sum is required [19]. Fig. 3.2 illustrates the schematic symbol for the electronic gate which implements this function and its truth table. Note that exclusive or, denoted by $\oplus$, is the Boolean function $x \oplus y = \bar{x}y + x\bar{y}$. In SSI (small scale integration) logic, the cost of four such gates is approximately 20¢. In LSI, the cost is much lower.



A	B	C
0	0	0
0	1	1
1	0	1
1	1	0

SYMBOL FOR EXOR AND TRUTH TABLE

FIG. 3.2



A SHIFT REGISTER COMPOSED OF D TYPE FLIP-FLOPS

FIG. 3.3

Another digital device of interest here is the shift register [19] consisting of a tandem connection of flip-flops which can store and shift streams of data under control of a clock. Fig. 3.3 illustrates a shift register. Here again, costs are low. MSI (medium scale integration) shift registers of up to 8 bits are available for under $1. MOS and CCD registers of lengths up to hundreds and thousands of bits are available for prices in the neighbourhood of $5 to $50. These component prices are being given here so the reader can judge for himself the inexpensive nature of many of the cryptographic processes to be described.

A widely used system for generating keys, enciphering, and deciphering is the linear binary sequential network composed of shift registers and exclusive or gates. Although, for simplicity this discussion is limited to modulo 2 networks and binary numbers, the same types of construction can be generalized to modulo p networks [20,21,22,23], and made to operate on groups of bits (i.e. bytes or characters) instead of individual bits. A general linear sequential binary network containing both feedback and feedforward taps on the shift register is illustrated in Fig. 3.4.

When specialized to feedback only, such networks are usually termed "sequence generators." Such networks can be designed to produce specific periodic sequences by choosing appropriate tap points on the shift register [24]. One form is called the "m-sequence" or pseudo-random

sequence generator. If the length of the shift register is N bits, the generator can be designed to produce a periodic sequence of period 2^N-1. The designs for many of these m-sequences have the interesting property that the number of "1s" and "0s" in the sequence differs by 1, i.e. there are an almost equal number of "1s" and "0s", and the occurrence of these "1s" and "0s" has a random nature if the probabilities of occurrence are calculated on a short term frequency basis. Hence the name pseudo-random sequence.

Since shift registers of lengths up to 2000 bits are available and are inexpensive it is quite feasible to generate sequences of length $2^{2000} - 1 \simeq 10^{602}$. Note that at a data rate of 9600 bps $\simeq 10^4$, the sequence takes $\simeq 10^{598}$ seconds or $\simeq 10^{588}$ years to repeat itself. For many practical purposes this sequence can be considered an "infinitely" long random sequence.

In the communications industry many m-sequences are specified as standards, for instance there is a CCITT standard 511 bit sequence for testing data sets, and a $2^{23}-1$ sequence is specified as a scrambling sequence in the new CCITT V.29, 9600 bps MODEM [25].

Fig. 3.5 illustrates the connections for a 511 bit m-sequence generator. The generator can be started at any state, except the all zero state, by preloading (seeding) the shift register with that state. The sequence is then

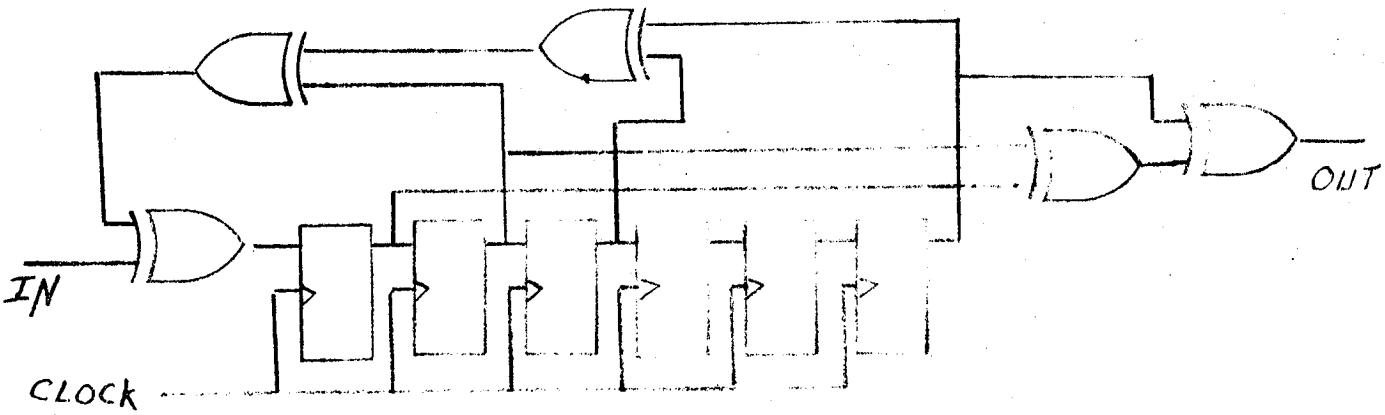


FIG. 3.4

GENERAL LINEAR BINARY SEQUENTIAL NETWORK

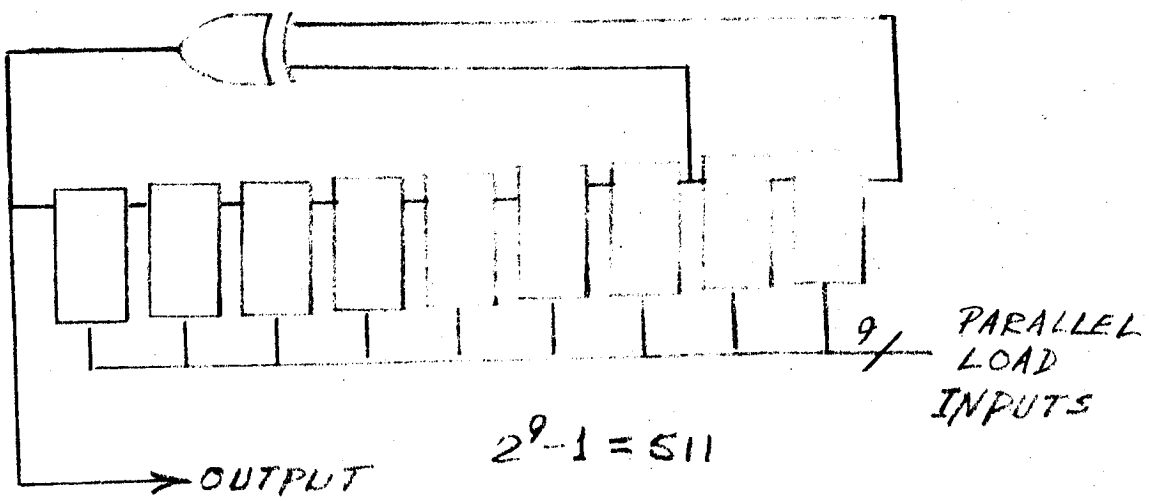


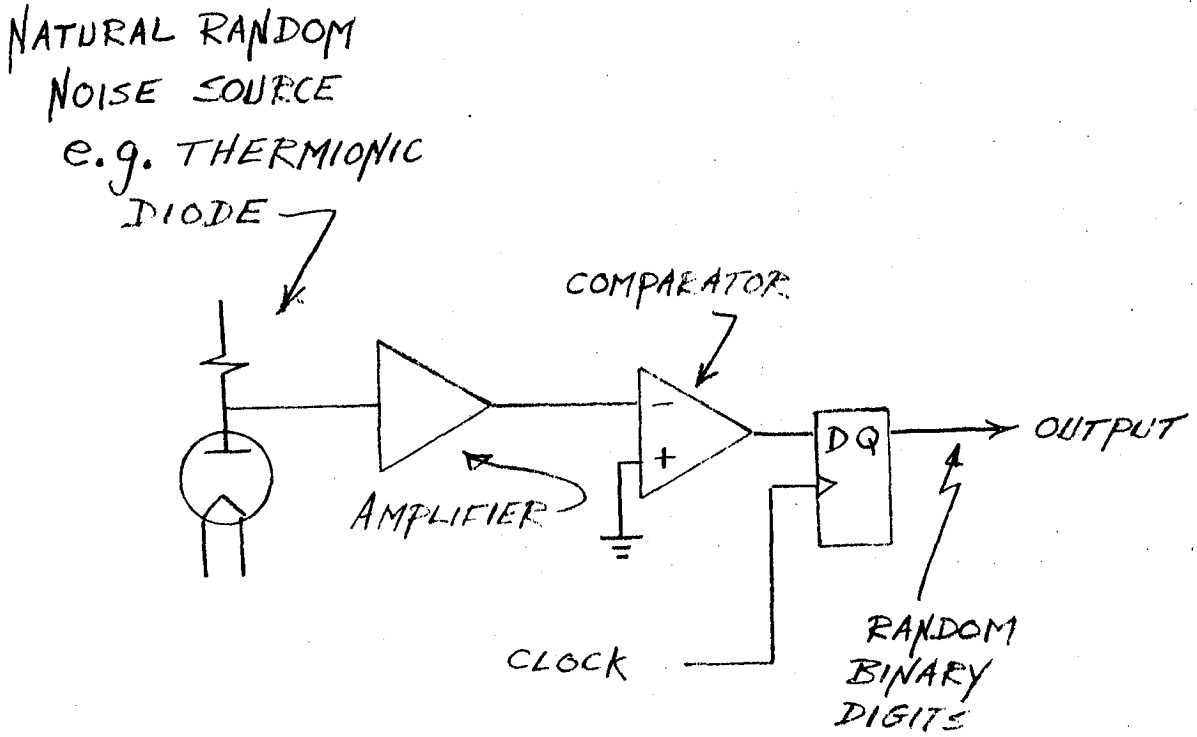
FIG. 3.5

A PRESETTABLE 511 BIT M-SEQUENCE GENERATOR

generated by clocking the shift register which causes it to shift. The sequence may then be obtained by tapping it off at the output of any shift register stage.

Truly infinite random sequences can be generated by utilizing a natural random process such as, the emission of radioactive particles from decaying radioactive material, the thermal shot noise of a vacuum doide, or the "Johnson" thermal noise of a resistor. The naturally generated noise is amplified, compared with a threshold and converted to an electrical binary data stream by a clocked flip-flop as illustrated in Fig. 3.6. The random data stream could be recorded for future use. At least one company uses this technique for generating random cipher keys for paper tape operated cryptographic equipment. The operation of this system will be described later.

Returning now to cryptographic systems, Fig. 3.7 is a block diagram of a general private key secrecy system. The dotted lines on the "key channel" denote a secure channel. In practice this secure channel may be a special courier. (In diplomatic work, keys are often relayed by diplomatic couriers in locked self-destruct diplomatic attache cases.) In any case, it is assumed that the secure channel is not accessible by the "enemy." The plaintext is encyphered by the crypto device using the key. The ciphertext is transmitted over the public channel to the remote location. It is assumed that the enemy has access



GENERATING AN "INFINITELY" LONG RANDOM BINARY DATA STREAM
(SUITABLE FOR USE WITH A "ONE TIME PAD" CRYPTO)

FIG. 3.6

to the public channel and can record the ciphertext for his attempts at cryptanalysis. The ciphertext is received at the remote location and deciphered by the remote crypto using the private key to produce the plaintext again. Such systems usually have elaborate alarms to indicate any faults which might cause the crypto device to transmit "in clear". Such alarms usually also stop the "in clear" transmission.

Turning to some specific examples using the devices discussed above, the simplest and most elegant system is the so called "one time pad" system illustrated in Fig. 3.8 Here, the key is an infinite random binary stream, the enciphering device is a single exclusive or gate which adds (modulo 2) the key to the plaintext to produce the ciphertext. The deciphering device is again an exclusive or gate which again adds the key to the ciphertext to produce the plaintext. In practice, this system will require some additional logistical support in the form of synchronization devices, and methods for distributing the key. Note that if synchronization is lost, so that the received key is delayed relative to the ciphertext, the message cannot be deciphered. Elaborate synchronization systems are in use to avoid this possibility.

It turns out that this simple "one time pad" system is unconditionally secure, a fact proven mathematically by Shannon [14] and for which the details will be sketched later. Note that the key must be truly random and no part

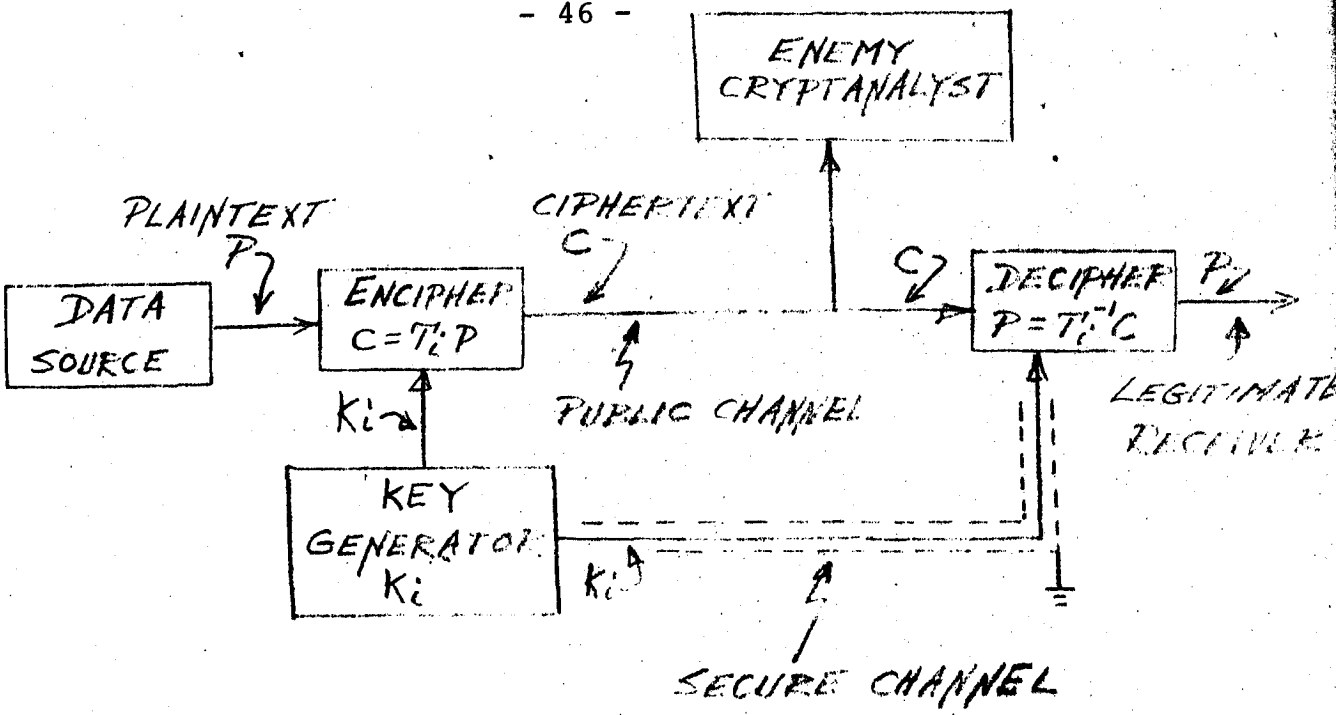


FIG. 3.7

A GENERAL PRIVATE KEY CRYPTOSYSTEM

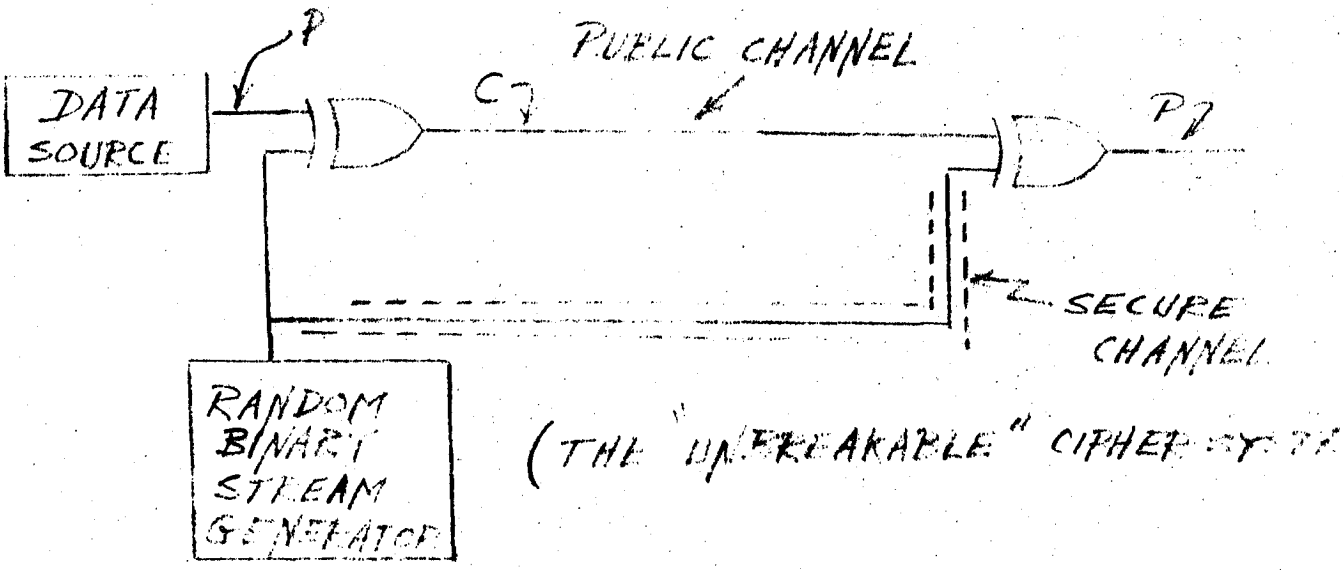


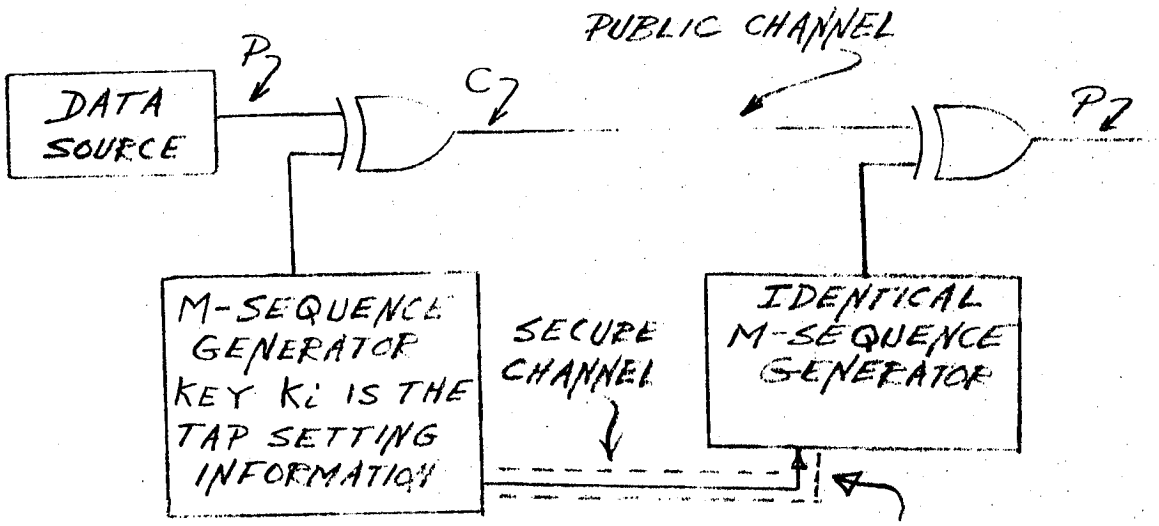
FIG. 3.8

THE "ONE TIME PAD" SYSTEM

of it may ever be used again to encode plaintext. The papertape system mentioned earlier for generating random tapes actually destroys the key tape as it is fed into the enciphering and deciphering machines to ensure that it will never be reused [1]. Note also that the capacity of the secure key channel must equal that of the public channel, i.e. the amount of key generated equals the amount of cipher traffic. These deficiencies are a small price to pay for an "unbreakable" cipher. No cryptanalysis can ever enable the enemy to determine the plaintext with absolute certainty.

A less secure system can be obtained as illustrated in Fig. 3.9. Here the truly random keys are replaced by m-sequence or pseudo-random generators. In this case, the capacity of the secure channel can be less than that of the "one time pad" system since the only information that has to be transmitted to the remote crypto is the feedback tap settings (only a few are required) and the "seed" or starting state for the generators. Often the "seed" is included with the ciphertext and sent over the public channel, and the "seed" is changed with each separate message sent. In this case, the seed is termed the "message key" and the process of receiving it and loading it into the crypto becomes a synchronizing procedure called priming.

This system is not unconditionally secure since the key is periodic (although it may be of great length) and



ONLY THE TAP SETTINGS AND INITIAL STARTING STATE ARE SENT ON THE SECURE CHANNEL. THUS, THE CAPACITY OF THE SECURE CHANNEL CAN BE A LOT LESS THAN THE CAPACITY OF THE PUBLIC CHANNEL.

FIG. 3.9

A SIMPLIFICATION AND WEAKENING OF THE ONE TIME PAD SYSTEM

given enough ciphertext traffic a statistical analysis can uncover the key and enable the enemy to read the traffic. Such systems usually use very long keys and make provisions for changing the keys (tap settings) which can be done weekly, daily, hourly, etc. The advantage of this system over the one time pad system is logistical in that the key distribution is simplified. Such a system can be more easily used in a broadcast or switched type system with many users. Pseudo-random generators using non-linear processes [26,27] can be substituted for the m-sequence generators to produce even longer and more random keys.

An even less secure system termed an auto-key or self synchronizing scrambler can be constructed. With this system, the synchronization required by priming the receiving crypto with the "seed" or message key is eliminated [28,29,30]. Such scramblers are used in adaptively equalized data MODEMs to scramble or randomize the transmitter signal so that the adaptive equalizer can maintain a good "average" equalization. These scramblers are specified by standards in some cases viz. the CCITT V.29 9600 bps MODEM standard [25].

Fig. 3.10 illustrates a self-synchronizing scrambler or auto-key crypto. Note that the ciphertext message itself acts as the key. The only secure information required is the position of the feedback taps on the transmit scrambler.

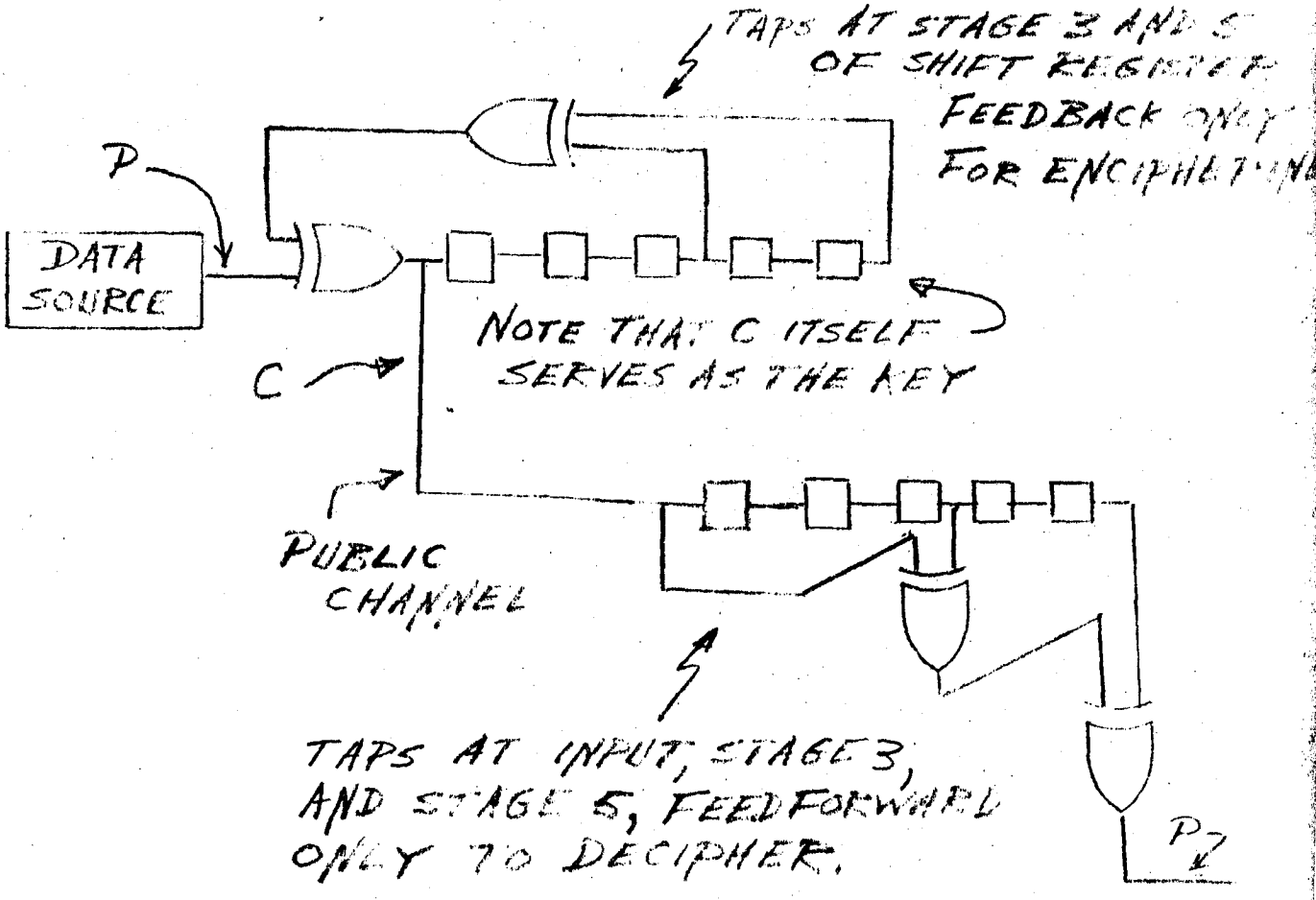


FIG. 3.10

THE SELF-SYNCHRONIZING SCRAMBLER OR AUTO-KEY SYSTEM

(NO SECURE CHANNEL REQUIRED)

The descrambler is not a feedback device, but is a feed forward device having its feed forward taps in the same position as the feedback taps on the scrambler. The reader can convince himself that this cascade system of "matching" feedback and feed forward linear networks results in a transparent path. If any errors occur in the ciphertext their effect is felt at the receiver as long as they are in the descrambler shift register, a period of about N bits. Fairly simple methods of determining the feedback taps on the scrambler are available [31].

3.3 The Shannon Theory of Cryptography (Private Key Cryptosystems)

In 1949 a declassified paper by Claude E. Shannon [14] detailed the communication theory of secrecy systems. Using concepts from his Information Theory, Shannon set up a rigorous mathematical basis for studying crypto systems. He introduced a numerical measure D for the redundancy of a data source or language (here the digitized voice) [32,33]. Here, D measures, in a sense, how much a language can be reduced without losing any information. Recall from section 2 that vocoders can "reduce" the bit rate of "good" quality digitized voice from 64 kbps (PCM) to about 2400 bps. In theory even further reduction is possible. Thus the vocoders or CODECs are removing redundancy from the voice. This process is termed "source encoding." Shannon showed that redundancy is an important concept

in secrecy systems. In fact, it is the residual redundancy in ciphertext that enables the cryptanalyst to gain information from statistical studies of the ciphertext. Clearly, the "one time pad" removes all redundancy from the ciphertext data stream.

Shannon looks on enciphering as an invertible transformation T_i corresponding to a certain key denoted by K_i. The deciphering operation is the inverse transformation T_i^{-1}. Thus, if the plaintext is denoted by P and the ciphertext by C then the operation of enciphering is to compute

$$C = T_i P$$

and the operation of deciphering is to compute

$$P = T_i^{-1} C.$$

The enemy cryptanalyst has available the ciphertext C and knows the set of possible enciphering transformations $\{T_i\}$, as well as the statistical properties of the source P. The object of the secrecy system being to prevent the enemy from determining a particular P. The enemy is also prevented from learning K_i, which is transmitted on the secure channel.

When a message is sent, Shannon assumes that a particular key K_i and transformation T_i will be chosen from the available set with a certain a priori probability. Similarly the message P to be transmitted will be chosen from a known set with a certain a priori probability.

These a priori probabilities represent the enemy cryptanalysts a priori knowledge of the situation. When the enemy intercepts the ciphertext C, he uses it to calculate (Bayes Theorem) the a posteriori probabilities of the various messages and keys which might have produced C. The calculation of these a posteriori probabilities, a statistical exercise in applying Bayes Theorem, constitutes cryptanalysis.

Shannon gives an example. For a simple monalphabetic substitution cipher in English, there are 26! transformations, which are equilikely yielding a priori probabilities of 1/26!. It is assumed that the cryptanalyst knows the a priori probabilities of English text. Once the cryptanalyst receives C his probabilities change. Clearly his a posteriori probabilities could depend some way on the size (number of letters N) of C. The message P with the highest a posteriori probably constitutes the cryptanalyst's "best" estimate of P. A quantity H(N), the equivocation, is defined which measures statistically how "near" the average ciphertext C of N letters comes to allowing the cryptanalyst a unique solution. Using these techniques, Shannon gives a formula for the "unicity" distance which determines how many letters N of C are required for a unique solution. The unicity distance is given by

$$\text{unicity distance} \simeq H(K)/D$$

For the simple example here, $H(K) \simeq \log_{10}(26!) \simeq 20$ and $D \simeq 0.7$ for English. Thus the unicity of a simple substitution cipher is about 30 letters, which is about the number one finds in the "anagram" puzzles published in the daily newspaper which most people can "break" with a little effort.

Using these methods, Shannon's results can prove that the "one time pad" is unconditionally secure (unicity tends to infinity) and can compute the unicity for various enciphering schemes. Thus the relative merits of various crypto algorithms can be compared in a quantitative manner. Of course in digitized voice one must know the redundancy D of the digit stream [33], but note that unicity increases with decreasing D so that operation of a vocoder through a crypto scheme increases the unicity (hence security) relative to say simple PCM.

3.4 New Directions in Cryptography (Public Key Cryptosystems)

Very recently, a novel type of cryptosystem has been proposed [34,35] and a flurry of activity surrounding it has appeared in the technical literature [36,37,38,39,40]. This system differs from the Shannon system in that the keys are made public and actually are listed in a public directory. The system has a number of unique features, and one possible fatal flaw. The scheme shows promise

and will be briefly outlined here although it seems not to have been put to practical use at this date. The system is not unconditionally secure, but rather is thought to be computationally secure, which means that extraordinary amounts of computation are required for cryptanalysis. Thus, it will not replace the "one time pad" as the ultimate in secrecy systems.

The new system proposed by Diffie and Hellman depends on the existence of certain "trap door" or "one way" functions which are defined using some conjectures from a relatively new branch of mathematics in the theory of automata called "complexity theory" or the theory of computational complexity.

Complexity theory deals with the subject of the difficulty of solving problems. Problems are generally solved by one of two methods, either guessing the answer (results depend on luck) or performing a prescribed algorithm. An algorithm is a procedure set out which, if followed, leads to the solution of the problem. It is interesting that some problems can be proved to be "unsolvable", that is, it can be proved that no algorithms exist for their solution, and the only method available is guessing. The celebrated Turing machine halting problem is just such a problem [41].

In the area of solvable problems, complexity theory is interested in determining the degree of difficulty in-

volved in executing the algorithm for solution. One of the activities in this area is attempting to prove that certain problems do not have "easy" algorithms. If it can be proven that a problem has no "easy" algorithms then a definite statement can be made about the amount of time and effort involved in solving the problem.

The degree of difficulty involved in executing an algorithm is measured in terms of the number of operations and amount of storage required to execute the algorithm. To date, solvable problems have been classified as P (for polynomial) when the number of operations required rises no faster than some polynomial in a linear measure of the problem size, say the number of letters N in a ciphertext, and as NP (for non deterministic polynomial) when the number of operations rises faster than a polynomial, say exponentially.

It is conjectured that there exists a subclass of NP problems now called "NP Complete" which are unique in that if an algorithm of complexity P is discovered for one of these problems then they are all solvable by an "efficient" algorithm. To date, these NP-Complete problems have resisted all attempts at finding an efficient algorithm and it is generally believed that they in fact belong to the class NP. If an efficient algorithm (still an open problem) is discovered, then P and NP are identical and only two classes remain, the unsolvable and P solvable. It is

generally believed that this will not be so, and today, if a problem is proven to be NP-Complete then it is assumed to be a lost cause to try and discover an efficient algorithm for it. In addition, there are problems in NP but which have not been proven to be NP-Complete. One of these is the problem of composite numbers, that is the problem of determining the factors of large numbers. This problem is the key to one of the proposed "trap door" functions.

With this background aside, the public key cryptosystem can be described [34]. The central idea in these systems is to eliminate the requirement for the second "secure" channel of the classical systems. Here, the keys can be transmitted on public channels "in clear", while only the deciphering algorithm remains secret and in the private possession of the ciphertext recipient.

Here cipher transformations T_i and their inverses T_i^{-1} are chosen from a set $\{T_i\}$ and their corresponding keys K_i. The T_i must have the following properties: each T_i^{-1} must be computationally infeasible to compute from T_i without knowledge of K_i; for every K_i it is feasible to compute T_i and T_i^{-1} from K_i; T_i and T_i^{-1} must be relatively easy to use.

Thus every pair T_i and T_i^{-1} in the cryptosystem must be such that the problem of computing T_i^{-1} from T_i belongs to the class NP defined earlier. Because of this property, the enciphering algorithms T_i can be made public and dis-

tributed to all possible receivers including enemies without compromising the security of the deciphering transformations T_i^{-1}. The functions T_i are termed "trap door" or "one way" functions due to the ease of computing T_i from T_i^{-1} and difficulty of computing T_i^{-1} from T_i.

The present research efforts [36,37,38] are directed at finding such suitable transformation pairs. Several of these have been proposed, and it has been mentioned [36] that patent action is being taken by the discoverers. However, a recent patent search reported in section 7 has not uncovered any applicable patent literature.

The system is depicted in Fig. 3.11, where we see that there is no requirement for an additional "secure" channel. Clearly the logistical problems of secure distribution and synchronization of keys in the classical cryptosystems have been eliminated. The invention of public key cryptosystems is an engaging idea, however their ultimate security will remain undecided until certain problems in complexity theory have been resolved. As yet these systems do not seem to have been put into practical service, and this author has certainly been unable to uncover any documentary evidence of their use in secure digital voice applications.

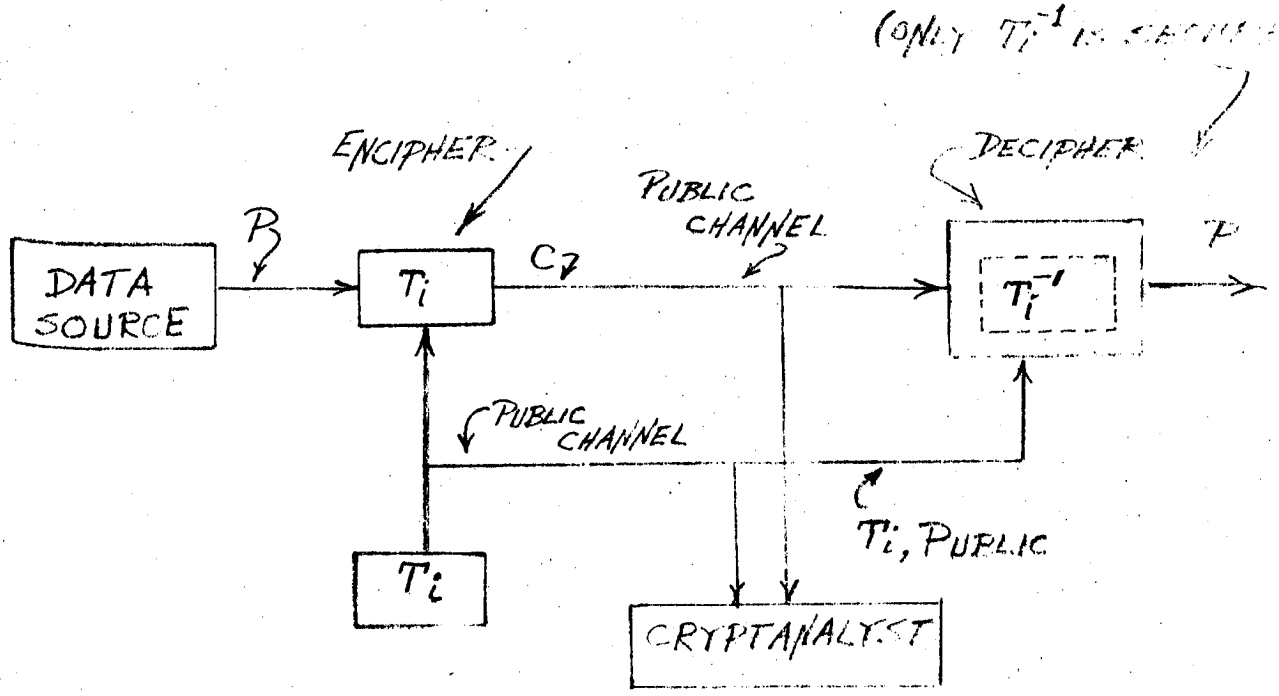


FIG. 3.11

A GENERAL PUBLIC KEY CRYPTOSYSTEM

3.5 Voice Encryption

After the above review of the theory of secrecy systems it is now possible to see its application to voice encryption. A secure voice system can be assembled by simply connecting in tandem one of the several voice digitizing systems, and processing the resulting digital data stream through a cryptosystem. Such a combination is called a digital secure voice terminal.

If the data output of the crypto is fed to a MODEM, the resulting analog signal can be easily passed over the public switched telephone network. Such a system is depicted in Fig. 3.12.

There are several possible variations on this system that are of interest to us in this study. First, as mentioned in section 2.4, a number of commercially available voice digitizers provide multiplexing capability so that one or more slow speed data terminals can be multiplexed in with the voice signal. Thus, the voice digitizer can be used for simultaneous voice and data transmission. If a crypto is attached to such a system, one obtains simultaneous secure voice and data. An additional complication is that modern high speed MODEMs are often equipped with multiplexers. For instance, there is a CCITT standard (V.29) which breaks a single 9600 bps data set into four channels which can run at 2400 bps each. In this case, additional data sources may

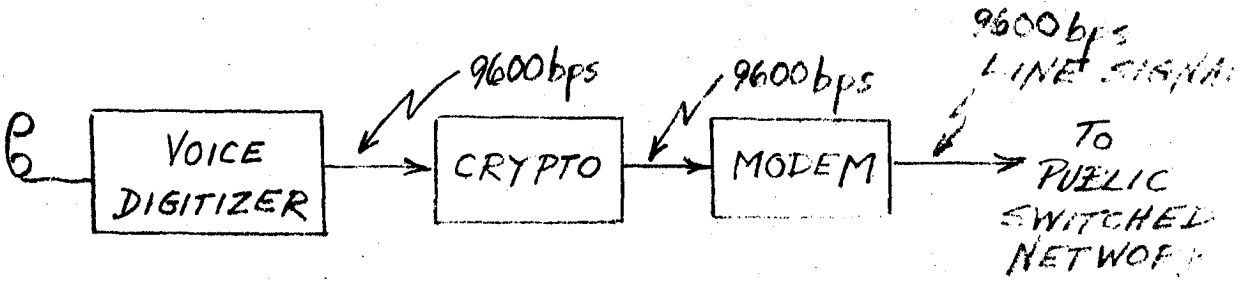


FIG. 3.12

SECURE DIGITAL VOICE ON THE PUBLIC NETWORK

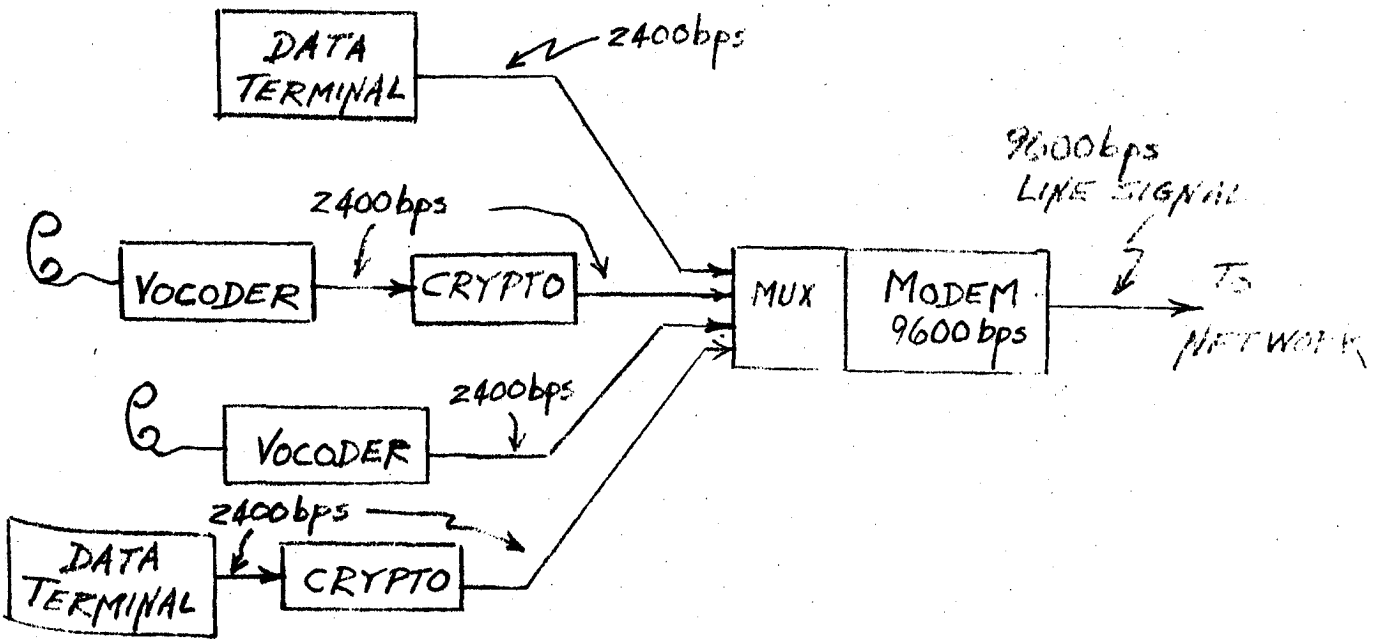


FIG. 3.13

A PUBLIC NETWORK CIRCUIT CARRYING A MIXTURE OF DATA, SECURE DATA, DIGITAL VOICE AND SECURE DIGITAL VOICE AT 9600 bps

be multiplexed in with secure voice. Fig. 3.13 illustrates an extreme scenario with a single 9600 bps MODEM transmitting a number of voice, data, secure voice and data, etc. signals over one public switched network channel. Clearly, the switched network channel is carrying both voice and data traffic simultaneously.

Another interesting scenario is the creation of a private secure voice network over a single public channel using switches (PBX) at either end as shown in Fig. 3.14 In this case, if a "one time pad" cryptosystem is in use, there is no way that the carrier could determine that his network was being put to such use.

3.6 Commercial Products, Costs and Summary

In this section several available commercial products for both data encryption and secure voice application are reviewed. Most available encryption devices which run synchronously at speeds greater than 2400 bps will be suitable for use with vocoders and CODECs in secure voice applications.

Datotek Inc. manufacture a crypto unit, the Datocoder, Model DS-138, Synchronous Data Scrambler. It can encrypt/decrypt synchronous data at rates up to 9600 bps in both half and full duplex modes. This unit makes use of a proprietary key generator (see the patent search information on Datotek in section 7). The operation of this

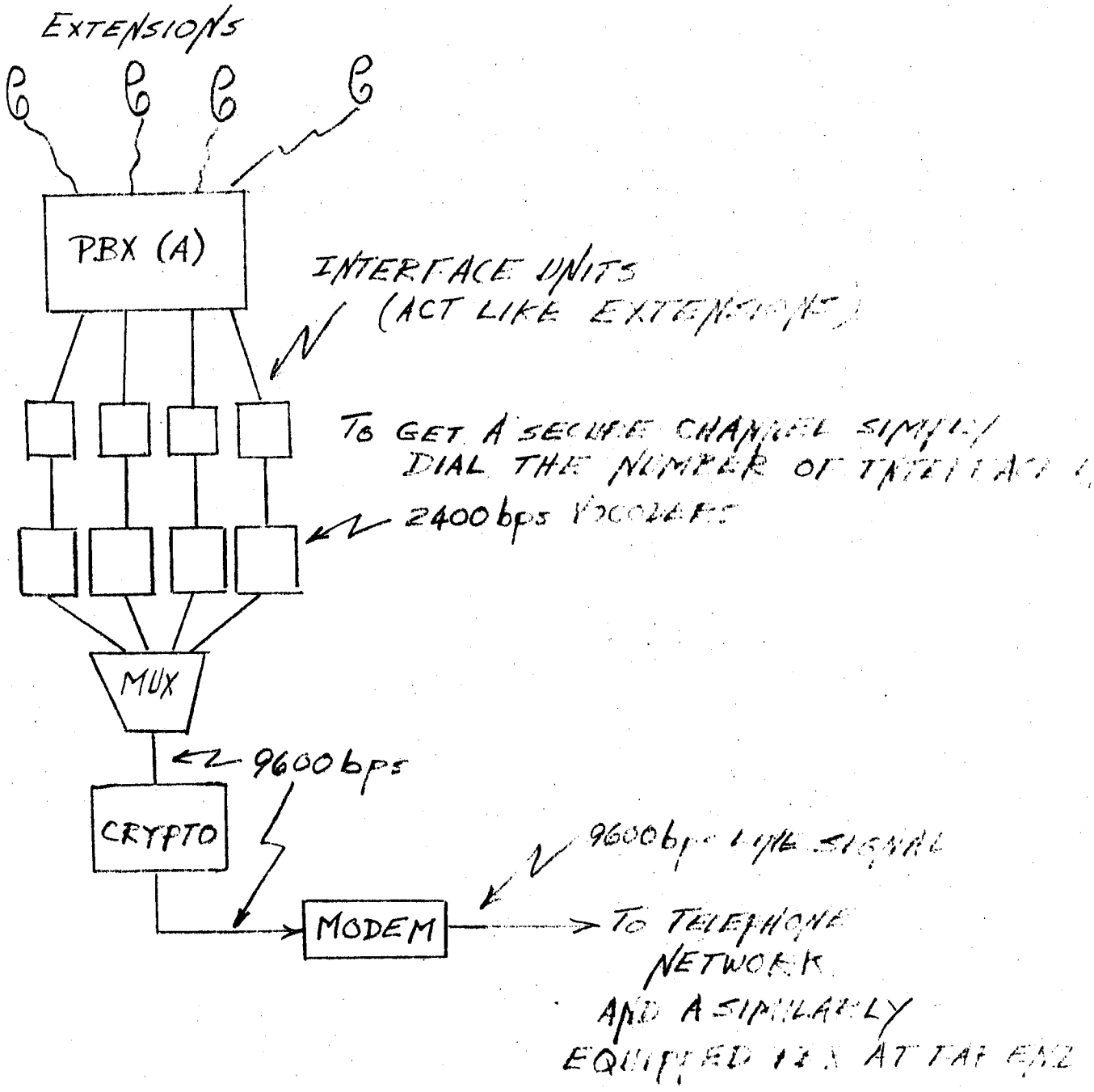
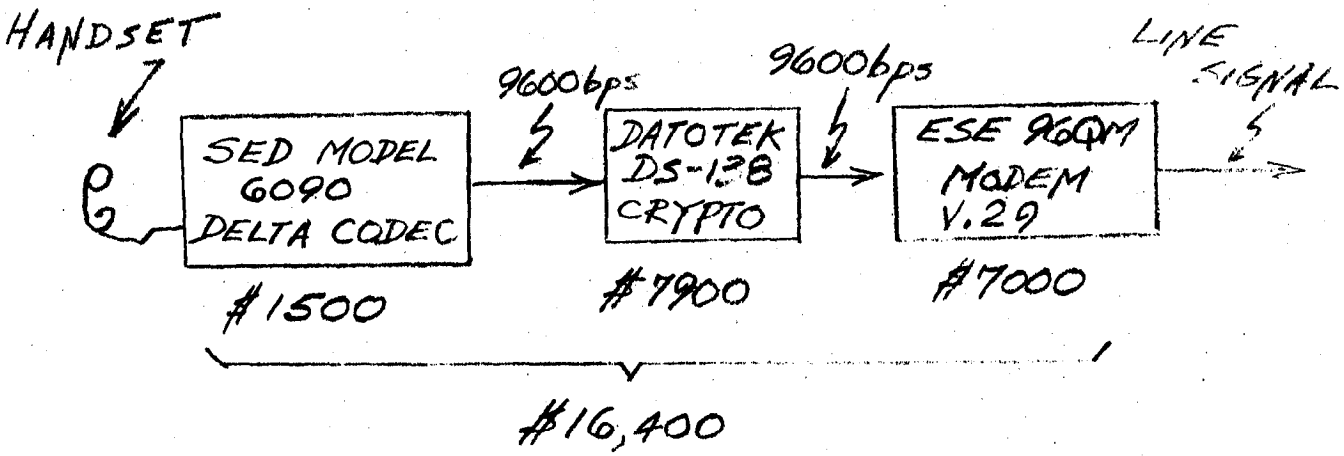


FIG. 3.14

USING PBX's TO CREATE A PRIVATE SWITCHED SECURE DIGITAL VOICE NETWORK

unit is automatic. At the time data transmission begins the unit enters a short synchronization sequence and thereafter ciphers all transmitted data. It is compatible with standard interfaces (RS232). Over 10^{52} different key settings or keys are available to the user. Its operation is independent of communications software protocol and transmission channel. It is desk mounted and weighs about 35 lbs. The price of the DS-138 in unit quantities is $7900 US as of February 1978. If the Datocoder DS-138 is combined with say the SED CODEC ($1500) described in the previous section, a secure voice terminal for communications quality voice results. The price of the combination is $9400. Further connecting the DS-138 to a 9600 bps MODEM suitable for switched network use ($7000) yields a complete secure voice system from handset to line at a cost of about $16,400. This setup is depicted in Fig. 3.15.

Technical Communications Corporation, manufacture a Model DPD 72/72A, which is a data privacy device or crypto with standard interfaces and operates in asynchronous or synchronous environments in either half or full duplex modes. The unit uses a non-linear autokey system and features unattended operation. The 72/A model has over 68 billion (US billion?) code selections available to the user. The Model 72A Full Duplex version is priced at $5450 US, February 1978. TCC have used this unit with



(ALL PRICES AS OF FEB 1979)

FIG. 3.15

A COMPLETE SECURE VOICE TERMINAL ASSEMBLED FROM COMMERCIAL PRODUCTS

the Time and Space Processing LPC vocoder described in the previous section. These two units could be interconnected at 2400 bps resulting in a complete high quality secure voice terminal including a 2400 bps MODEM for about $22,000. TCC will actually build custom secure voice terminals and deliver them completely packaged for about $25,000 to $35,000 depending upon options.

Motorola manufactures microprocessor based crypto equipment (either in card or stand alone form) which is marketed under the trade name Info Guard. The card cryptos use either the 6800 or 8080 processors, and Motorola will help purchasers to write their own crypto software. In addition, they manufacture stand alone units such as the Model 1100, and the Network Security Model 4100. The latter device includes RS232 interfacing, synchronous or asynchronous operation at speeds up to 56 kbps. The system is programmed to use the recent NBS crypto algorithm. The price is $2800, February 1978.

E-Systems manufactures a complete secure voice terminal called the VIP Voice Security Terminal. The voice digitizer used is the E-Systems VADAC 5 speech processor described in section 2; the crypto used is an OEM model purchased by E-Systems. The terminal has an optional MODEM and can operate at 2400/4800 bps. A fully equipped VIP terminal sells for about $30,000 per terminal in unit quantities, February 1978.

Several of the above manufacturers intimated to this author that they also have other (more secure?) crypto gear available which they cannot sell due to export restrictions on "strategic" devices. Perhaps they have military customers. In any case "one time pad" systems do not seem to be readily available, at least to this author, although such systems should not be too much more expensive. The key generating equipment is simple, and the key could be recorded on magnetic tape for use at the remote end just as is done for the Hagelin paper tape "one time pad" system described earlier.

At the present time, February 1978, it appears as if the cost of a complete secure voice terminal lies in the range of $15,000 to $35,000 depending upon the bit rate, voice quality, and level of security desired. These prices are small quantity prices in a low volume market. The prices for digitizing equipment has been projected into 1980-1985 in section 2. Again here in the crypto area it is impossible to get manufacturers to project prices (They have a vested interest in selling their equipment today!) However, from the introduction to this section it can be seen that many of the processes involved in electronic crypto are easily integrated so that if demand warrants it, complete LSI crypto units on a single IC chip could become available. In fact, Datotek manufactures a calculator-like device for encryption by hand from a key-board.

Certainly 2000 bit shift registers are now being sold in IC form at reasonable prices. Thus, in large volume, one can see crypto units in chip form selling for the price of the large LSI chips sold today, i.e. $100. Generally, crypto units are less expensive than vocoders due to their inherently simpler processing. Thus, combining the projected cost for voice digitizers ($500) with the projected cost of a crypto (say $250 including interfacing, etc.) results in a total cost of about $750 for a secure voice terminal in the period 1980-1985.

Of course, if demand does not develop, the cost of developing the LSI chips required will preclude such drastic price reductions. It is quite possible that such a demand will develop because of the present controversy surrounding the usurption of civil liberties and the invasion of personal privacy by both private and government agencies. Business and personal communicators may feel that $750 is a small price to pay for guaranteed privacy from wiretappers.

3.7 References

The following references are grouped into those quoted in the text, those of general interest, a selection of patents from the cross-indexed list of section 7, and a list of companies supplying data encryption equipment.

[1] David Kahn, The Code-Breakers, The Macmillan Company, New York, 1967.

[2] David Kahn, The Code-Breakers, Signet Paperback, New York, 1973.

[3] David Kahn, "Modern cryptology", Scientific American, Vol. 215, No. 1, pp. 38-46, July 1966.

[4] See U.S. Patent No. 4,070,693 in numerical list of section 7.

[5] See U.S. Patent No. 1,676,321 in numerical list of section 7.

[6] See U.S. Patent No. 3,991,271 in numerical list of section 7.

[7] See U.S. Patent No. 4,031,837 in numerical list of section 7.

[8] See U.S. Patent No. 3,991,271 in numerical list of section 7.

[9] Donn B. Parker, Crime by Computer, Charles Scribner and Sons, New YOrk, 1976.

[10] Bruce J. Walker and Ian F. Blake, Computer Security and Protection Structures, Dowden, Hutchinson and Ross Inc.,

[11] Horst Feistel, "Cryptography and computer privacy," Scientific American, Vol. 228, No. 5, pp. 15-23, May 1975.

[12] U.S. National Bureau of Standards (NBS DES) "Data Encryption Standard", a Federal Information Processing Standard, FIPS Publication No. 46, Jan. 15, 1977. (Available from the U.S. Govt. Dept. of Commerce, National Technical Information Service, Springfield, VA, 22151., or order directly from their sales desk at (703) 557-4650). Other FIPS publications of interest are FIPS Pub. No. 39, "Glossary for Computer Systems Security", Feb. 15, 1976 and FIPS Pub. No. 41, "Computer Security Guidelines for Implementing Privacy Act of 1974", May 30, 1970.

[13] Claude E. Shannon, "A mathematical theory of communication", BSTJ, Vol. 27, pp. 279-423, July 1948.

[14] Claude E. Shannon, "Communication theory of secrecy systems", BSTJ, Vol. 28, pp. 656-715, Oct. 1949.

[15] See U.S. Patent No. 1,416,765 of section 7.

[16] See U.S. Patent No. 1,479,846 of section 7.

[17] See U.S. Patent No. 1,555,042 of section 7.

[18] See U.S. Patent No. 1,686,585 of section 7.

[19] Herbert Taub and Donald Schilling, Digital Integrated Electronics, McGraw Hill, New York, 1977.

[20] D.A. Huffman, "The synthesis of sequential switching circtuis", J. Franklin Inst., March-April 1954, pp. 161-190, 275-303.

[21] E.F. Moore, Gedanken-Experiments on Sequential Machines, Automata Studies, Princeton University Press, Princeton, N.J., pp. 129-153, 1956.

[22] M. Phister, Logical Design of Digital Computers, John Wiley and sons, New York, 1958.

[23] See the "Sequential Transducer Issue", IRE Trans. on Circuit Theory, Vol. CT-6, No. 1, March 1959.

[24] S.W. Golomb, Shift-Register Sequences, Holden-Day, Inc., San Francisco, 1967.

[25] CCITT Recommendation V.29, approved in 1977.

[26] See U.S. Patent No. 3,911,216 of section 7.

[27] See U.S. Patent No. 3,657,476 of section 7.

[28] See U.S. Patent No. 3,925,611 of section 7.

[29] J.E. Savage, "Some simple self-synchronizing digital data scramblers," BSTJ, Vol. 46, No. 2, pp. 449-487, Feb. 1967.

[30] Benjamin Arazi, "Self synchronizing digital scramblers," IEEE Trans., Vol. COM-25, No. 12, pp. 1505-1507, Dec. 1977.

[31] See U.S. Patent No. 4,034,156 of section 7.

[32] C.E. Shannon, "Prediction and entropy of printed English," BSTJ, Vol. 30, pp. 50-64, Jan. 1951.

[33] B.G. Taylor, "Entropy of delta coded speech" Proc. IEE, Vol. 123, No. 8, pp. 743-751, Aug. 1976.

[34] Whitfield Diffie and Martin E. Hellman, "New directions in cryptography," IEEE Trans., Vol. IT-22, No. 6, pp. 644-654, Nov. 1976.

[35] Martin E. Hellman, "An extension of the Shannon theory approach to cryptography," IEEE Trans., Vol. IT-23, No. 3, pp. 289-294, May 1977.

[36] Martin Gardner, "Mathematical games. A new cipher that would take millions of years to break," Scientific American, Vol. 237, No. 2, pp. 120-124, Aug. 1977.

[37] Stephen C. Pohlig and Martin E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," IEEE Trans., Vol. IT-24, No. 1, pp. 106-110, Jan. 1978.

[38] R.L. Rivest, A. Shamir, and L. Adleman, "On digital signatures and public-kay cryptosystems," Dep. Elec. Engr. and Comp. Sci., MIT, Cambridge, MA, Tech. Rep. MIT/LCS/TM-82, Apr. 1977. (This memo can be obtained free of charge by writing Rivest and enclosing a 9 x 12 inch SASE with 35¢ postage)

[39] Harry R. Lewis and Christos H. Papadimitriou, "The efficiency of algorithms," Scientific American, Vol. 238, No. 1, pp. 96-109, Jan. 1978.

[40] A. Evans, W. Kantrowitz and E. Weiss, "A user authentication scheme not requiring secrecy in the computer," Comm of ACM, Vol. 17, pp. 442-445, Aug. 1974.

[41] Alan M. Turing, "On computable numbers, with an application to the entscheidungsproblem," Proc. Lon. Math. Soc., Series 2, Vol. 42, Parts 3 and 4, pp. 230-265, Nov.-Dec. 1936.

[42] S.C. Kak and N.S. Jayant, "On speech encryption using waveform scrambling," BSTJ, Vol. 56, No. 5, pp. 781-808, May-June 1977.

[43] Vera S. Pless, "Encryption schemes for computer confidentiality," IEEE Trans., Vol. C-26, No. 11, pp. 1133-1136, Nov. 1977.

[44] Horst Feistel, William A. Notz, and J. Lynn Smith, "Some cryptographic techniques for machine-to-machine data communications," Proc. IEEE, Vol. 63, No. 11, pp. 1545-1554, Nov. 1975.

U.S. Patents of Interest Selected from the Cross-Indexed Numerical List of Section 7.

3,911,216; 3,798,360; 3,798,359; 3,988,538; 4,034,156; 4,004,089; 3,983,326; 3,962,539; 3,958,081; 3,936,601; 3,934,078; 3,796,830; 3,700,806; 3,683,513; 3,657,476; 2,394,765; 2,139,676.

LIST OF COMPANIES
SUPPLYING ENCRYPTION EQUIPMENT

Acrodyne Data Devices Inc.,
1217 Summit Ave.,
Union City, NJ 07087
(201) 865-3220

Atlantic Research Corp.,
5390 Cherokee Ave.,
Alexandria, VA 20402
(703) 354-3400

Datotek Inc.,
13740 Midway Rd.,
Dallas, TX 75240
(214) 233-1030 Ms. Ray Layman

Digital Communications Corp.,
19 Firstfield Rd.,
Gaithersburg, MD 20760
(301) 948-0850

E-Systems Inc.,
Garland Division,
P.O. Box 6118,
Dallas, TX 75222
(214) 272-0515 Mr. Donald Fulghum

GTE Sylvania,
1800 N. Kent St.,
Arlington, VA 22209
(703) 841-9020

Harris Corp./Electronics Systems Division,
P.O. Box 37,
Melbourne, FL 32901
(305) 727-4130

Hughes Aircraft Co.,
5250 W. Century Blvd.,
Los Angeles, CA
(213) 670-1515

ITT/Data Equipment and Systems Div.,
E. Union Ave.,
E. Rutherford, NJ 07073
(201) 935-3900

Mitron Systems Corp.,
2000 Century Plaza,
Columbia, MD 21044
(301) 992-7700

Motorola Government Electronics Div.,
8201 E. McDowell Rd.,
P.O. Box 1417,
Scottsdale, AZ 85252
(602) 949-4735 Mr. James Booth

Technical Communications Corp.,
56 Winthrop St.,
P.O. Box 1070,
Concord, MA 01742
(617) 862-6035 Mr. Dennis King

4 DIGITAL VOICE ON DATA NETWORKS

4.1 Circuit Switched Networks

There appears to be no particular difficulty associated with the use of digital voice on circuit switched data networks, since the digital data may be transmitted continuously once a circuit is established. Data communications equipment (MODEMs) installed at either end of the circuit appear as digital ports to the data sources and sinks which are now vocoders or CODECs instead of the conventional data terminal equipment. As noted in an earlier section, many of the commercially available vocoders either have integral MODEMs or have provision for a MODEM as a user selected option. Thus, the use of circuit switched data networks for digital voice is an accomplished fact.

The only facet that needs to be considered here is the performance of the digital voice scheme in the presence of data errors. In fact, digital voice is more highly tolerant to high error rates than pure data communications systems. Typical data error rates on circuit switched networks are 10^{-5}, a level that is just tolerated in data communications, whereas most vocoders produce acceptable speech at rates as high as 10^{-2}, and rates as high as 10^{-1} can be tolerated in bursts [1,2,3].

It should be noted that since normal human speech contains idle periods that amount to about 60 to 65% of a

call duration, the use of a data circuit for a single digital voice link might not be considered an efficient use of such a resource. At least one company [4] has proposed and is actively marketing a system to connect two PBXs using TSIUs (telephone system interface units) to provide links between 2400 bps vocoders and the telephone system. Such a system depicted in Fig. 3.14 allows the user to construct his own private switched secure digital voice network using a single public switched network data circuit. The TSIUs allow normal call dialing and routing functions between the two PBXs. Note that crypto units can be placed at either end to service up to four extensions, using a single 9600 bps data circuit.

4.2 Packet Switched Networks

On the surface there appears to be several difficulties associated with applying digital voice to a packet switched network. Most of these potential difficulties are due to the packetized nature of the communications channel which does not form a continuous path from source to sink, but rather transmits the data in short "packets" throughout the network in a "store and forward" fashion. Some of the potential problems for voice transmission in this environment are:

- The transmission delay of each packet is random.
- There is a fixed delay encountered in "filling" packets with speech.

- Packets can be received out of order.
- Packets can be lost or duplicated.
- Overhead in the form of destination, acknowledgement and error correction information is included in each packet.

The first four points raised here imply that a system for speech packet reassembly at the receiving terminals must be employed. This system must look after the housekeeping requirements of receiving the packetized digital speech and assembling the received packets in their correct temporal order before outputting the digital voice data to a digital voice terminal. In addition, some strategy regarding lost or missing packets must be employed.

The last point regarding overhead must enter into economic considerations since clearly the throughput and, hence, cost will be a strong function of the information data to overhead data ratio for packets. Also, since digital voice is more tolerant to errors than machine traffic it may be useful to consider the deletion of error control information from digital voice packets.

At least three experiments on packet switched digital voice have been reported [4 , 5 , 6]. The ARPANET experiment reported by Gold details some of the results. It is pointed out in that report that letting O be the number of overhead bits in a packet, L be the total packet length, R be the bit rate of the digital voice, D be the delay to

fill a packet, and C the channel capacity needed to transmit complete packets, then

$$D = \frac{L - O}{R}$$

is the delay taken to fill a packet, and

$$C = \frac{RL}{L - O}$$

is the channel capacity required to transmit those packets.

In some cases, the delay D can be considerable, and cause user annoyance in full duplex voice communication. For example, at R = 2.4 kbs (for a good quality vocoder like the VADAC 5) L = 1024 (for say the Bell Datapak service) with O ≃ 200, the delay D obtained is 343 msec which is comparable to the delay on satellite channels. Here, the capacity required is C ≃ 3kbs. The packet filling delay above in conjunction with the transmission delay is probably unacceptable. Gold reports that on ARPANET, 95% of the random transmission delays were 350 msec or less, and 99% were 520 msec or less. Thus, one could choose a fixed delay of about 520 msec at the receiving terminal to allow packet reassembly with the assurance that only 1% of the packets will be lost. Adding this to the above 343 msec yields an overall delay of about 870 msec in the voice path. This is probably unacceptable to the general public, but may be quite acceptable to some users.

The delays mentioned above can be reduced by increasing R, which requires a larger capacity C, or by decreasing L-O, again requiring a larger capacity.

An alternative to the above trade-off situation is to capitalize on the relatively large percentage (60 to 65%) of idle time on a voice circuit much as is done in TASI (time assigned speech interpolation) systems [7]. Here, as described for TI-NET [4] as implemented at Carleton University, the data formatting processors which must be employed for speech packet reassembly, are able to make use of indications from the voice digitizer of busy and idle periods to reduce the required capacity C, thus allowing a larger R and consequently smaller delay D. A similar scheme has been recently proposed by Webber et. al. [6].

The experiments reported by Gold on using ARPANET for digital voice and the other reports quoted here indicate that by using the proper speech packet preparation and reassembly equipment (perhaps only implemented as software in the packet network node processors) digital voice in the packet switched environment will be quite feasible.

For the present, any users contemplating such use for commercially available packet services must provide their own formatting and reassembly processors which will add to their communications cost, although the incremental cost compared to the present cost of a secure digital voice

terminal (≃ $35,000) may be negligible. Fig. 4.1 illustrates how such a data formatting/reassembly processor would be connected between the voice digitizer and MODEM, or digital port.

4.3 References

[1] P. Noll, "Effects of channel errors on the signal-to-noise performance of speech-encoding systems," BSTJ, Vol. 54, No. 9, pp. 1615-1636, Nov. 1975.

[2] J. Yan and R.W. Donaldson, "Subjective effect of channel transmission errors on PCM and DPCM voice communication systems," IEEE Trans., Vol. COM-20, No. 3, pp. 281-290, June 1972.

[3] Donald P. Fulghum, "A secure voice communications system," paper available by writing E-Systems Inc., Garland Div., Garland, Texas. Attn., D. Fulghum.

[4] Donald P. Fulghum, "Voice data compaction and privacy communications systems," paper available by writing E-Systems Inc., Garland Div., Garland, Texas. Attn., D. Fulghum.

[5] Bernard Gold, "Digital speech networks," Proc. IEEE, Vol. 65, No. 12, pp. 1636-1658, Dec. 1977.

[6] S.A. Webber, C.J. Harris, and J.L. Flanagan, "Use of variable-quality coding and time-interval modification in packet transmission of speech," BSTJ Briefs, BSTJ, Vol. 56, No. 8, pp. 1569-1573, Oct. 1977.

[7] Bullington and Fraser, "Engineering aspects of TASI," BSTJ, Vol. 38, No. 2, pp. 353-364, March 1959.

[8] L.G. Roberts, "Data by the packet," IEEE Spectrum, Vol. 11, No. 2, pp. 46-51, Feb. 1974.

[9] C.E. White, "Packet switching for fast and secure data," Telecommunications, Int. Ed., Vol. 12, No. 1, pp. 33-38, Jan. 1978.

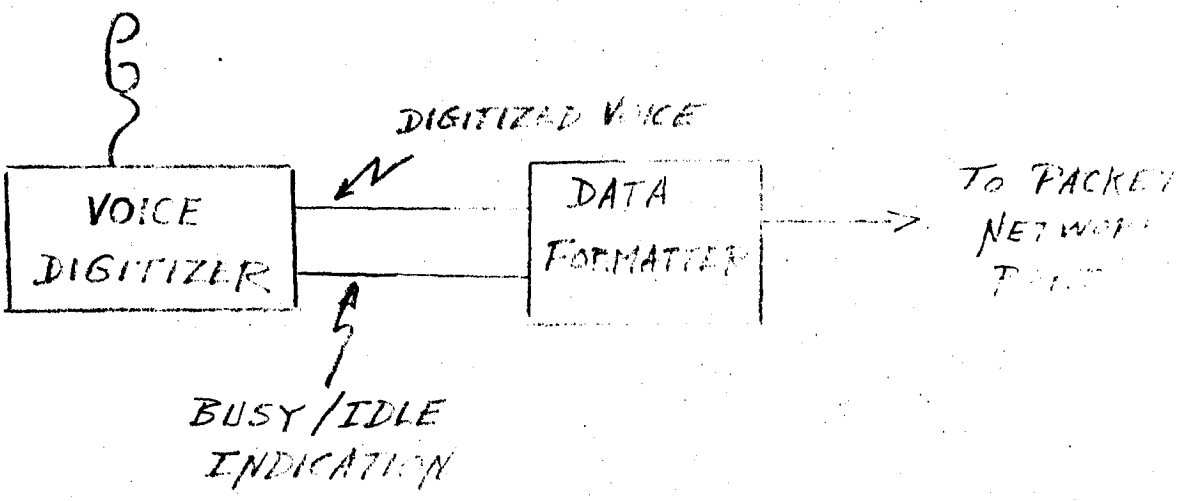


FIG. 4.1

A DATA FORMATTING PROCESSOR TO INTERFACE A DIGITAL VOICE TERMINAL TO A PACKET NETWORK

5 IDENTIFICATION OF SIGNALS CARRYING VOICE

5.1 Introduction

Turning now to the central problem of this study, the question of identifying those circuits at the interconnection of a digital and public switched network which are carrying digital voice, it is useful to study the type of analog signals available to the proposed monitoring system. The circuits which are available are analog pairs at a switching center or central office. These pairs are carrying voice frequency (audio) signals which lie roughly in the band of 300 Hz to 3300 Hz. These circuits are of nominal 600 ohm impedance and must be connected to both the data MODEMs, which are receiving and transmitting the voice frequency line signals, and the proposed monitoring equipment. In what follows it will be assumed that the operators of the proposed monitoring equipment have the facility for making the required connections without degrading the circuit performance.

5.2 MODEM Line Signals

From previous considerations of voice digitizing equipment it was noted that, at present, acceptable digital voice requires bit rates of at least 2400 bps, and because of the use of the public switched network, data rates in excess of 9600 bps are not of interest at the present time.

Thus, the line signals that the monitoring equipment will have to observe are those generated by voice frequency MODEMs which operate at speeds between 2400 bps and 9600 bps. It will be assumed that the operator of the monitoring equipment knows the types of MODEMs in use since the MODEMs in question will actually be installed on the premises of the operator (the public switched network carrier).

Fortunately, due to standards, and the finite number of commercial MODEM manufacturers, there are only a finite number of such MODEMs in use. By consulting a typical trade guide [1], one finds that there are approximately 30 different manufacturers of such MODEMs, and as many types of MODEMs. In practice, only about 10 of these are in widespread use.

Typical MODEMs of this group perform similar kinds of operations to generate their voice frequency line signals. The serial digital data stream (or streams if the MODEM is fitted with a multiplexer) is encoded into multilevel pulses, perhaps scrambled by an autokey scrambler (similar to the autokey crypto devices described in section 3), bandlimited, and used to modulate a carrier in some manner. These processes lead to very complex line signals. In practice the higher speed MODEMs which include adaptive equalizers and therefore scramblers to ensure a uniform line spectrum have line signals which "sound" like "white noise". That is the human ear cannot tell the difference between the MODEM line

signal and a bandlimited white noise source. This characteristic is of course independent of whether the digital data stream is digitized voice or machine generated data.

All of these MODEMs must also transmit some kind of timing information so that the MODEM receivers can regenerate the data timing and carrier frequency information. Some of these MODEMs transmit the timing information continuously while transmitting data, and they can resynchronize from the line signal if synchronization is lost. Other types transmit synchronizing signals only during a "start up" or training mode. In these types, synchronization once lost cannot be regained without a new training sequence transmission from the MODEM transmitter.

A wiretapper or monitor wishing to examine the data signals which generated these MODEM line signals must perform the same operation provided by the MODEM receivers on the line signals. This is exactly the operation which will be proposed for a "practical" monitoring system.

5.3 Wiretapping and the Wiretap Channel

Some recent results of Wyner and others on the so-called "wiretap channel" appear to have some realtionship to this work [2 , 3 , 4]. The wiretap channel is similar to a broadcast channel, and typically the situation is as illustrated in Fig. 5.1. Here the wiretapper is eavesdropping on a main channel and there exists two information paths or

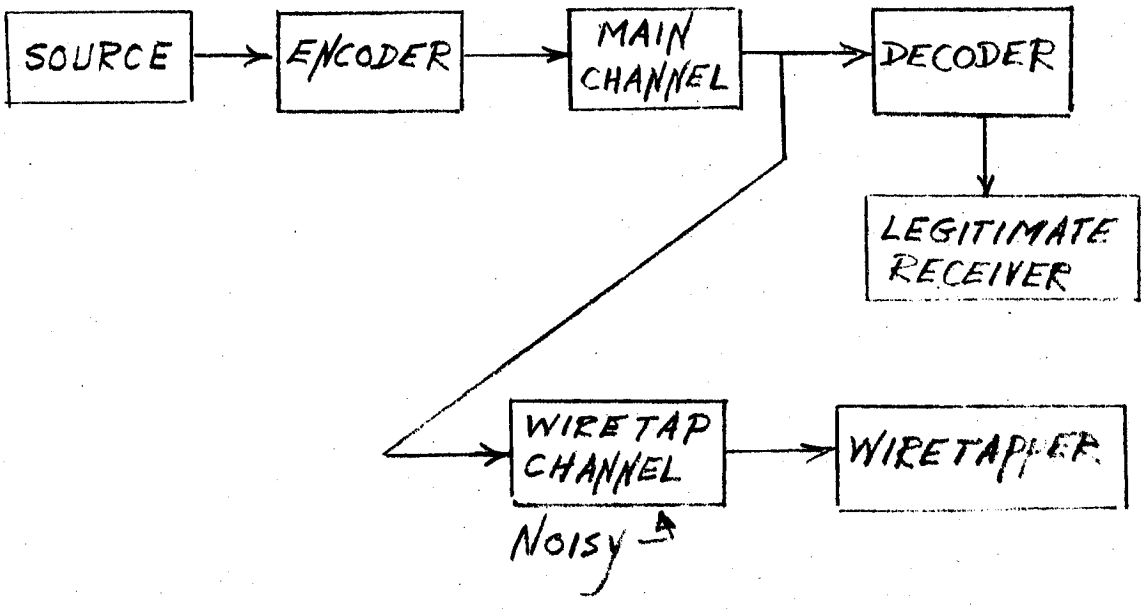


FIG. 5.1

THE WIRETAP CHANNEL

channels. One channel, the main channel, runs from the source to the legitimate sink or receiver, the second channel, the wiretap channel, consists of the path through the main channel and then through a wiretap channel to the wiretapper. The object of Wyner's work is to maximize the information rate over the main channel, while simultaneously minimizing it over the wiretap channel. The wiretapper is assumed to know the encoding schemes used at the transmitter and legitimate receiver and is handicapped only by the greater noise present in his received signal. Note that the objective here is the same as that for cryptography, however, the technique for achieving privacy is different. Wyner has shown that it is possible to encode in such a manner as to prevent the wiretapper from gaining any information, and perfect secrecy can be achieved.

Since Wyner's results depend upon the fact that the wiretappers signal is more "noisy" than the legitimate receiver's signal this result is not useful to the problem at hand. This is because, in the monitoring scheme projected by this study, the wiretapper (monitor) will have access to the signal before it traverses the network, thus the wiretapper's signal will in all probability be less noisy than the signals received by the legitimate remote receivers.

5.4 Monitoring the Non-Secure Scenario

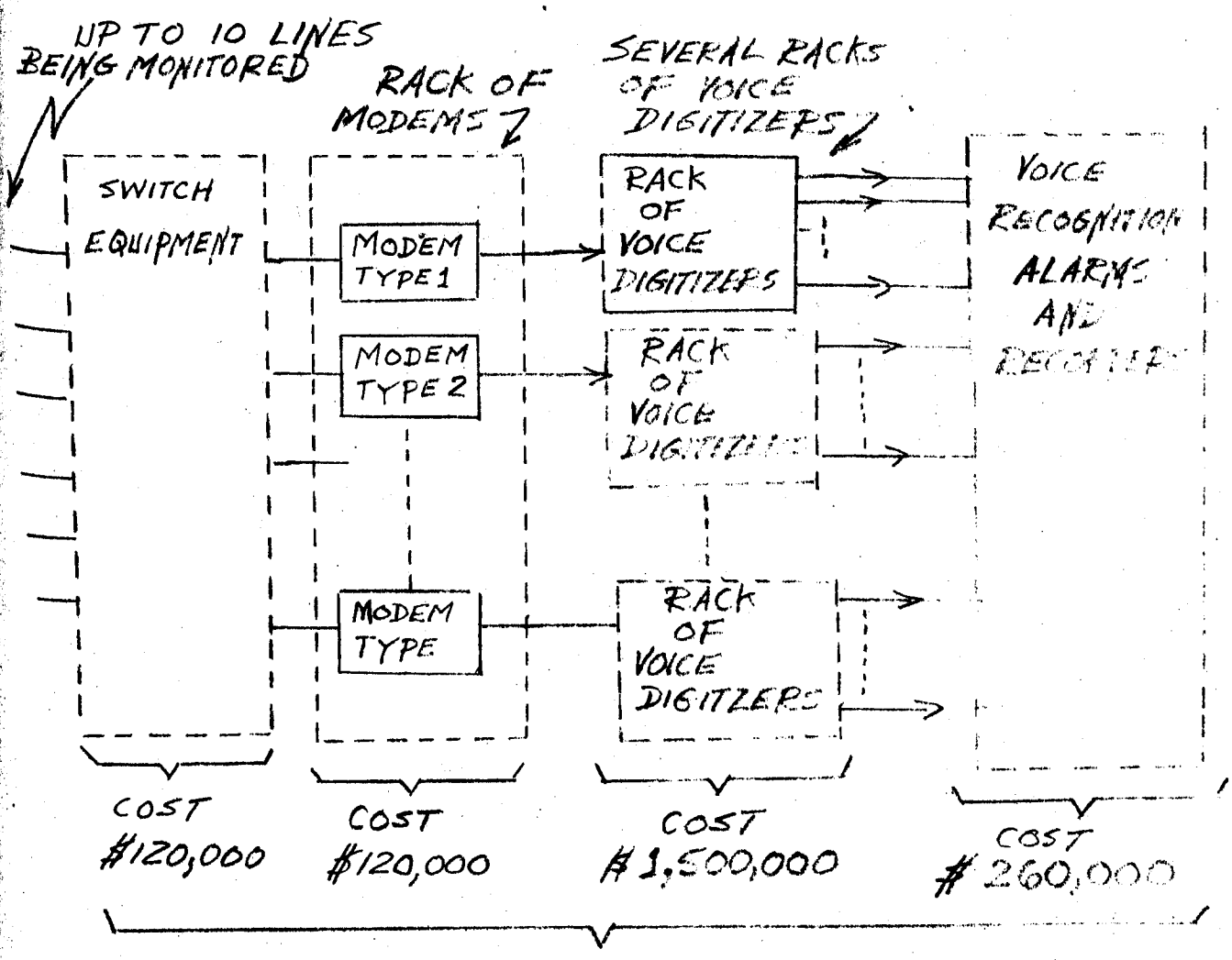
The non-secure scenario is the scenario of Fig. 1.1 without the crypto devices. That is, users are making use of an interconnection between a digital network and the public switched network to transmit digital voice without encryption. The object of this section is to estimate the costs of any practical monitoring device which can determine unambiguously those circuits carrying digital voice.

A very pragmatic approach will be taken to this problem, and an estimate of a practical monitoring system will be found in the form of an upper bound. The problem could be approached as a signal analysis problem involving a device which samples the line signals and passes the samples to a general purpose signal processing computer which makes use of Fast Fourier Transforms and statistical methods to analyze the line signals. Such an approach does not lend itself well to making estimates and in all probability would lead to a system of greater cost and complexity than the method to be proposed here.

Of course, it will be difficult in general to demodulate line signals generated by special purpose or proprietory MODEMs since the line signal formats then would be unknown and, as usual, very similar in nature to a noise source. Thus, any proposed monitoring scheme will have great difficulty on circuits using unknown or specially modified MODEMs. For instance, even with a standard MODEM

such as the CCITT V.29 9600 bps type which has a prescribed self-synchronizing scrambler/descrambler, it is a simple matter of reconnecting a couple of wires to modify the MODEM such that it is incompatible with all others of the same type and very difficult for a monitor to unscramble. If such special MODEMs were installed by the user, the monitoring task would become very difficult.

Supposing that the digital voice circuits are using standard MODEMs (perhaps supplied by the carrier) known to the carrier operating the monitoring equipment, a design for such a monitor can be outlined as follows. The "front end" of the monitor depicted in Fig. 5.2 consists of a rack of MODEMs of the known types. As mentioned previously there are only a finite set of these, say 15 different types. Taking a conservative estimate of about $8000 per MODEM this represents a total cost of about $120,000. This bank of MODEMs would be connected to the circuits being monitored, probably in a sequential manner by some type of switching mechanism connected to the lines. It would probably suffice to monitor each circuit for say a three minute period once every half hour, which would enable the monitor to "watch" ten active circuits. Of course, if more circuits were to be monitored the amount of equipment required would be increased. Let us estimate that the cost of switch gear to connect the lines to the bank of MODEMs is no greater than the bank of MODEMs, an additional $120,000.



A PROPOSED "PRACTICAL" MONITORING SYSTEM USING "OFF THE SHELF" SUBSYSTEMS

FIG. 5.2

NOTE: THIS SYSTEM IS NOT SUITABLE FOR MONITORING SECURE VOICE CIRCUITS

At the digital ports of the MODEMs, which are eavesdropping on the circuits, would be connected a bank of vocoders and CODECs for decoding the possible digital voice signals. Again here by economic necessity only a finite set of commercial voice digitizing equipment needs to be considered. The problem here being that the carrier operating the proposed monitor does not know which of the commercially available voice digitizers the user has connected and so must provide a bank of such equipment for each MODEM digital port. Thus assuming an average cost of voice digitizers as described in section 2, to be $10,000 and a total of about 10 different voice digitizers, results in a cost of about $100,000 per MODEM, with 15 different MODEMs, the total cost of voice digitizers would come to about $1,500,000.

Thus, a total cost for a monitoring equipment to monitor say 10 active circuits would be about $1,740,000. Of course, there will also be required some recording equipment to record the voice outputs of the digitizers which may or may not be decoding voice depending upon whether the circuit is being used to transmit voice or data. In addition, some type of voice recognition equipment could be installed which would give an alarm and turn on a recorder if voice-like signals were detected. Such equipment is known to be in certain types of communications equipment but is probably not commercially available as off-the-shelf

equipment. Thus one should allow about $260,000 for the development and installation of this equipment.

All of these considerations lead to an estimate of about $2,000,000 as the captial cost of the monitoring equipment depicted in Fig. 5.2. The operating cost would involve the full time effort of a combined maintenance man/operator at about $25,000 per annum including overhead.

Thus at an initial outlay of about $2,000,000 and a per annum expense of about $25,000 a digital voice monitoring station capable of monitoring say 10 circuits could be set up. It should be noted, that to ensure "complete" coverage the carrier would have to set up one of these systems at every switching center or central office at which the proposed network interconnections are to be accomplished. This large expense does not take into consideration the fact that the digital voice users may be utilizing crypto devices in the "worst" scenario, or multiplexing voice and data in the same digital streams.

5.5 Monitoring the Secure Scenario

In the secure scenario, the digital voice users avail themselves of crypto equipment, which as outlined in section 3 costs presently in the neighbourhood of about $10,000 per unit, but which is rapidly becoming more economical and widespread.

One could expand the monitoring system just described by attaching all known crypto equipment to the outputs of the voice digitizers. This, however, is of no use since the keys would be unknown to the monitoring agencies, and a general ciphertext-only cryptanalysis attack would have to be performed on each voice digitizer output. As shown in section 3 the users could easily be using a "one-time-pad" crypto which is known to be unbreakable by any crypt-analysis method. Thus the construction of a "practical" device to monitor the secure scenario is a fruitless effort since it can easily be defeated by any determined user of a secure voice terminal!

5.6 References

[1] 1977 Handbook and Buyers Guide, published by Tele-communications, Vol. II, No. 13, July 1977.

[2] A.D. Wyner, "The wire-tap channel," BSTJ, Vol. 54, No. 8, pp. 1355-1387, Oct. 1975.

[3] Aydano B. Carleial and Martin E. Hellman, "A note on Wyner's wiretap channel," IEEE Trans., Vol. IT-23, No. 3, pp. 387-390, May 1977.

[4] S.K. Leung-Yan-Cheong, "On a special class of wiretap channels," IEEE Trans., Vol. IT-23, No. 5, pp. 625-627, Sept. 1977.

6 CONCLUSIONS

Good quality voice digitizing equipment is commercially available today. Crypto equipment is also commercially available. The present cost of setting up a telephone quality secure digital voice terminal including a MODEM is about $35,000. A communications quality secure terminal could be set up for about $10,000. The costs of such terminals will decrease with demand. The technology is available today for constructing such terminals for costs in the neighbourhood of about $750. Such costs could be realized if demand warrants the development of the LSI circuits to implement the terminals.

Digital voice has been demonstrated in both the circuit and packet switched environments, the latter environment probably will require the development of special digital voice packet formatting processors. These processors may eventually be incorporated into the packet network node processors.

The capital cost of a monitoring system to monitor about 10 lines for possible digital voice use in the absence of crypto units is estimated at about $2,000,000. Many such units would be required, one for each network interconnection center.

In the case of users electing to use crypto devices, the cost of a practical monitoring system would be unbounded and this author considers it ludicrous to

even consider such a facility, since by means of a well known crypto technique, the "one-time-pad", the monitor can be rendered useless. In fact, the mere possibility that users might incorporate crypto units in their voice terminals forces one to conclude that there is no practical reason to consider even the monitor system described for the non-secure voice scenario.

7 RESULTS OF PATENT SEARCH

7.1 Introduction

In the course of preparing this study, a patent search was undertaken to ensure that the results reflected the state-of-the-art. The areas of voice digitization, encryption and secure voice have a voluminous patent literature. The patent literature appears to be more extensive in this area than the journal literature, especially in the area of cryptography.

The results of the patent search, represented by the patents listed in this section, comprise only about one fourth of the related patents found by this author. Those listed here were deemed to be the most directly related.

The patents listed in numerical order cover both of the fields in this study, namely digitized voice and encryption or some combination of both. The numerical listing also includes other patents cited by those listed which may or may not appear in this listing. Those citation could be used for further searching of related areas. Note that the patents found include some from as far back as 1882 and up to February of 1978. Many of the older ones have been included for their historical interest.

Note that in the references of the individual sections of this study the reader is referred to the numerical list of this section to avoid duplication of the patent references. These forward references are noted by

asterisks so that the reader can easily find those referred to in the main body of the study.

Also in this section is included an alphabetical listing of patentees or inventors which is cross-indexed to the numerical listing.

A third indexing in terms of the major assignees listed on the face of the patents was compiled. From this listing one can determine the companies most active in this area, and the number of patents they hold. It is interesting to note that many of the commercial firms supplying equipment listed in sections 2 and 3 do not appear here! This perhaps suggests that there is still further information held by companies in the nature of trade secrets that is not available to the general public.

Copies of patents listed here are available from the Commissioner of Patents and Trademarks, Washington, D.C., 20231, by simply writing and asking for the patent by number. The fee is 50¢ US per patent copy, postage paid.

7.2 NUMERICAL LIST OF RELATED U.S. PATENTS

1. A.F. and B.F. Johnson, "Apparatus for preparing and transmitting secret telegraphic messages," U.S. Pat. No. 253,061., Field 178-22, Jan. 31, 1882.

2. R.E. Pierce, "Secret signalling system," U.S. Patent No. 1,312,574., Field 178-22, Aug. 12, 1919.

3. R.D. Parker, "Ciphering and deciphering mechanism," U.S. Pat. No. 1,320,908., Field 178-22, Nov. 4, 1919, Ass. to A.T. and T.

4. G.C. Cummings, "Telegraphy," U.S. Pat. No. 1,352,116., Field 178-22, Sept. 7, 1920, Ass. to Western Electric.

5. L.F. Morehouse, "Ciphering system," U.S. Pat. No. 1,356,546., Field 178-22, Oct. 26, 1920, Ass. to A.T. and T.

6. A.J. Eaves, "Secret telegraphic system," U.S. Pat. No. 1,356,701., Field 178-22, Oct. 26, 1920, Ass. to Western Electric.

* 7. G.S. Vernam, "Ciphering device," U.S. Pat. No. 1,416,765., Field 178-22, May 23, 1922, Ass. to A.T. and T.

8. E.F.W. Alexanderson, "Radiosignaling system," U.S. Pat. No. 1,426,944., Field 178-22, Aug. 22, 1922, Ass. to General Electric.

9. R.D. Parker, "Ciphering machine," U.S. Pat. No. 1,442,819., Field 178-22, Jan. 23, 1923, Ass. to A.T. and T.

10. David E. Branson, "Secret signaling system," U.S. Pat. No. 1,470,594., Field 178-22, Oct. 16, 1923. Ass. to A.T. and T.

* 11. G.S. Vernam, "Ciphering device," U.S. Pat. No. 1,479,846., Field 178-22, Jan. 8, 1924, Ass. to A.T. and T.

12. Harry Pfannenstiehl, "Enciphering and deciphering mechanism," U.S. Pat. No. 1,491,358., Field 178-22, Apr. 22, 1924, Ass. to Western Electric.

13. A.G. Damm, "Production of ciphers," U.S. Pat. No. 1,502,376., Field 178-22, July 22, 1924.

14. A.R. Molins, "Secret system for radiotelegraphy," U.S. Pat. No. 1,505,055., Field 178-22, Aug. 12, 1924.

15. W.F. Friedman, et. al., "Secret signaling system employing apparatus for automatically enciphering and deciphering messages," U.S. Pat. No. 1,516,180., Field 178-22, Nov. 18, 1924.

16. A.U. Harper, "Secret communication system," U.S. Pat. No. 1,529,786., Field 178-22, Mar. 17, 1925. Ass. to A.T. and T.

* 17. G.S. Vernam, "Transmitting handwriting and pictures," U.S. Pat. No. 1,555, 042., Field 178-22, Sept. 29, 1925, Ass. to A.T. and T.

18. L.M. Potts, "Secret system of telegraphy," U.S. Pat. No. 1,558,280., Field 178-22, Oct. 20, 1925, Ass. to A.T. and T.

19. L.F. Morehouse, "Ciphering and deciphering device," U.S. Pat. No. 1,568,991., Field 178-22, Jan. 12, 1926, Ass. to A.T. and T.

20. O.B. Blackwell, et. al., "Secrecy communication system," U.S. Pat. No. 1,598,673., Field 178-22, Sept. 7, 1926, Ass. to A.T. and T.

21. R.V.L. Hartley, "Signaling method and system," U.S. Pat. No. 1,605,023., Field 178-22, Nov. 2, 1926, Ass. to Western Electric.

22. E. Belin, "Secret message transmitting system," U.S. Pat. No. 1,657,366., Field 178-22, Jan. 24, 1928.

* 23. A. Carpe, "Secrecy signaling system," U.S. Pat. No. 1,676,321., Field 178-22, July 10, 1928, Ass. to A.T. and T.

* 24. G.S. Vernam, "Telegraph cipher system," U.S. Pat. No. 1,686,585., Field 178-22, Oct. 9, 1928, Ass. to A.T. and T.

25. A.G. Damm, "Apparatus for transmitting and receiving telegraphic messages in code," U.S. Pat. No. 1,715,904., Field 178-22, June 4, 1929.

26. W. Korn, "Device for coding and decoding," U.S. Pat. No. 1,733,886., Field 178-22, Oct. 29, 1929.

27. R.H. Ranger, "Secret transmission system," U.S. Pat. No. 1,794,389., Field 178-22, Mar. 3, 1931, Ass. to RCA.

28. Parker Hitt, "Ciphering and deciphering apparatus," U.S. Pat. No. 1,848,291., Field 178-22, Mar. 8, 1932, Ass. to International Communications Laboratories.

29. Francoise Cartier, "Secret telegraphy system," U.S. Patent No. 1,868,967., Field 178-22, July 26, 1932.

30. W. Broertjes, "Method of maintaining secrecy in the transmission of wireless telegraphic messages," U.S. Pat. No. 1,869,659., Field 178-22, Aug. 2, 1932.

31. J.H. Smart, "Automatic secret telegraph system," U.S. Patent No. 1,900,772., Field 178-22, Mar. 7, 1933.

32. J.H. Hammond, Jr., "Secret television," U.S. Pat. No. 1,910,540., Field 178-22, May 23, 1933.

33. A. Jipp, et. al., "Secret telegraph system," U.S. Pat. No. 1,912,983., Field 178-22, June 6, 1933.

34. Franz Wrede, "Method and means for establishing secret communication," U.S. Pat. No. 1,945,014., Field 178-22, Jan. 30, 1934.

35. J.I. Bellamy, "Cryptographic system and apparatus," U.S. Pat. No. 1,953,918., Field 178-22, April 10, 1934., Ass. to Associated Electric Laboratories.

* 36. W.F. Friedman, "Cryptographic apparatus," U.S. Pat. No. 2,139,676., Field 178-22, Dec. 13, 1938., Ass. to U.S. Govt., Secy. of Navy.

37. J.B. Walker, "Means for forming and decoding secret messages," U.S. Pat. No. 2,151,452., Field 178-22, Mar. 21, 1939.

38. R.E. Mathes, "Secrecy system for telegraphy," U.S. Pat. No. 2,175,847., Field 178-22, Oct. 10, 1939., Ass. to RCA.

39. D.B. Perry, "Secret signaling system," U.S. Pat. No. 2,265,120., Field 178-22, Dec. 2, 1941., Ass. to A.T. and T.

* 40. B.C.W. Hagelin, "Ciphering and deciphering mechanism," U.S. Pat. No. 2,394,765., Field 178-22, Feb. 12, 1946.

41. J.A. Spencer, "Secrecy system for telegraph circuits," U.S. Pat. No. 2,397,057., Field 178-22, Mar. 19, 1946, Ass. to RCA.

42. J.A. Spencer, "Single channel secrecy device," U.S. Pat. No. 2,397,058., Field 178-22, Mar. 19, 1946., Ass. to RCA.

43. E.W. Bemis, "Teletypewriter secrecy system," U.S. Pat. No. 2,401,454., Field 178-22, June 4, 1946., Ass. to A.T. and T.

44. E.O. Gammell, "Teletypewriter secrecy system," U.S. Pat. No. 2,401,474., Field 178-22, June 4, 1946., Ass. to A.T. and T.

45. E.O. Gammell, "Teletypewriter secrecy system," U.S. Pat. No. 2,401,475., Field 178-22, June 4, 1946., Ass. to A.T. and T.

46. M.L. Greene, "Teletypewriter secrecy system," U.S. Pat. No. 2,401,477., Field 178-22, June 4, 1946., Ass. to A.T. and T.

47. W.B. Martin, "Secret signaling system," U.S. Pat. No. 2,401,494., Field 178-22, June 4, 1946., Ass. to A.T. and T.

48. R.E. Pierce, et. al., "Secrecy cipher system," U.S. Pat. No. 2,401,507., Field 178-22, June 4, 1946., Ass. to A.T. and T.

49. L.A. Briggs, et. al., "Enciphering and deciphering system," U.S. Pat. No. 2,401,855., Field 178-22, June 11, 1946., Ass. to RCA.

50. R.E. Mathes, "Enciphering and deciphering system," U.S. Pat. No. 2,401,877., Field 178-22, June 11, 1946., Ass. to RCA.

51. C.S. Szegho, "Secrecy communication system," U.S. Pat. No. 2,401,985., Field 178-22, June 11, 1946, Ass. to Rauland Corp. of Chicago.

52. R.M. Hicks, "Secret telegraph system," U.S. Pat. No. 2,403,280., Field 178-22, July 2, 1946., Ass. to Teleregister Corp.

53. C.I. Cronburg, "Enciphering and deciphering system," U.S. Pat. No. 2,403,888., Field 178-22, July 9, 1946, Ass. to A.T. and T.

*54. H.S. Black, et. al., "Pulse code modulation communication system," U.S. Pat. No. 3,020,350., Field 179-1.5E, Feb. 6, 1962, Ass. to Bell Telephone Labs., (Cites: 2,272,070; 2,007,809.)

55. H.G. Lindner, "Security communication system," U.S. Pat. No. 3,025,350., Field 179-1.5E, Mar. 16, 1962, Ass. to U.S. Govt., Secy. of Army, (Cites: 2,777,897; 2,658,189; 2,603,714; 2,580,148; 2,521,690.)

* 56. W.M. Goodall, "Cipher system for pulse code modulation communication system," U.S. Pat. No. 3,071,649., Field 179-1.5E, Jan. 1, 1963, Ass. to Bell Telephone Labs, (Cites: 2,427,687; 2,438,908; 2,446,613; 2,449,819; 2,482,544.)

57. M.R. Schroeder, "Speech privacy system," U.S. Pat. No. 3,328,526., Field 179-1.5E, June 27, 1967, Ass. to Bell Telephone Labs, (Cites: 3,280,258; 3,055,980; 2,976,491.)

58. G. Guanella, "Process for concealing communications signals," U.S. Pat. No. 3,536,833., Field 179-1.5E, Oct. 27, 1970, (Cites: 3,243,507; 3,077,518; 3,071,649; 2,777,897.)

59. B.F. Hagersten, "Ciphering machine," U.S. Pat. No. 3,557,307., Field 178-22, Jan. 19, 1971, (Cites: 3,038,028.)

60. C.S. Hetlevik, "Method of automatic enciphering and deciphering of signal pulses," U.S. Pat. No. 3,602,645., Field 178-22, Aug. 31, 1971, (Cites: 3,036,156.)

61. Robert C. Woodhead, "Secret signaling system," U.S. Pat. No. 3,603,734., Field 178-22, Sept. 7, 1971, Ass. to Canadian Govt., (Cites: 2,517,587; 2,510,054; 2,479,338; 2,426,255; 2,406,790; 2,406,350; 2,402,058; 2,401,406.)

62. D.E. Andrews, Jr., et. al., "Secure communications system," U.S. Pat. No. 3,614,316., Field 178-22, Oct. 19, 1971, Ass. to U.S. Govt., Secy. of Navy, (Cites: 3,158,864; 2,870,431; 2,796;602; 2,553,284; 2,444,452.)

63. Donald F. Wolper, "Telegraph secrecy system," U.S. Pat. No. 3,627,928., Field 178-22, Dec. 14, 1971, Ass. to Litton Systems, (Cites; 3,038,028.)

64. William V. Braun, et. al., "Digital privacy system," U.S. Pat. No. 3,639,690., Field 178-22, Feb. 1, 1972, Ass. to Motorola, (Cites: 3,507,980; 3,506,783; 3,307,648; 3,202,764.)

65. Gustav Guanella, "Message scrambling apparatus for use in pulsed signal transmission," U.S. Pat. No. 3,651,261., Field 178-22, Mar. 21, 1972, (Cites: 3,341,659; 3,289,082; 3,244,808; 3,133,991; 3,078,344; 3,067,280; 3,201,515; 3,148,333; 3,040,192; 2,696,599.)

* 66. Howard H. Aiken, "Cryptography," U.S. Pat. No. 3,657,476., Field 178-22, Apr. 18, 1972.

67. Emanuele Angeleri et. al., "Message scrambler for PCM communications system," U.S. Pat. No. 3,659,046., Field 178-22, (Cites: 3,427,399.)

68. Kurt Ehrat, "Circuit for generating a series of cipher pulses," U.S. Pat. No. 3,678,198., Field 178-22, July 18, 1972, (Cites: 2,995,624.)

* 69. Sture Nyberg, "Apparatus for automatically enciphering and/or deciphering a text consisting of multidigit coded characters," U.S. Pat. No. 3,683,513., Field 178-22, Aug. 15, 1972. (Cites: 3,309,694; 2,750,586.)

70. Barrie O. Morgan, et. al., "Digital cryptographic system and method," U.S. Pat. No. 3,686,631., Field 178-22, Feb. 25, 1975, Ass. to Datotek, (Cites: 3,751,646; 3,562,711; 3,594,500; 3,555,255; 3,515,805.)

71. James A. McDonald, "Signal coding and decoding system," U.S. Pat. No. 3,688,193., Field 179-1.5E, Aug. 29, 1972, Ass. to Motorola, (Cites: 3,536,833; 3,328,526.)

* 72. Jean-Pierre Vasseur, "Key generators for cryptographic devices," U.S. Pat. No. 3,700,806., Field 178-22, Oct. 24, 1972, (Cites: 3,515,508.)

73. Frank H. Gentges, "Method and apparatus for encoding and decoding analog signals," U.S. Pat. No. 3,746,799., Field 178-22, July 17, 1973, Ass. to U.S. Govt., Secy. of Navy, (Cites: 3,507,980.)

74. James W. Crimmins, et. al., "Security phone," U.S. Pat. No. 3,775,562., Field 179-1.5R, Nov. 27, 1973, Ass. to Data Transmission Sciences Inc., (Cites: 3,299,215; 3,114,800; 2,785,231.)

75. George E. Goode, et. al., "Digital data ciphering technique," U.S. Pat. No. 3,781,472., Field 178-22, Dec. 25, 1973, Ass. to Datotek, (Cites: 3,546,380; 2,406,829; 2,897,268; 2,690,475; 2,898,402; 2,993,089; 3,522,374; 2,951,120.)

76. George E. Goode, et. al., "Random digital code generator," U.S. Pat. No. 3,781,473., Field 178-22, Dec. 25, 1973, Ass. to Datotek, (Cites: 3,506,783; 3,557,307; 3,170,033; 3,051,783; 3,038,028.)

77. H.C. Schroeder, "Parallel data scrambler," U.S. Pat. No. 3,784,743., Field 178-22, Jan. 8, 1974, Ass. to Bell Telephone Labs, (Cites: 3,711,645.)

* 78. John Lynn Smith, "Recirculating block cipher cryptographic system," U.S. Pat. No. 3,796,830., Field 178-22, Mar. 12, 1973, Ass. to IBM. (Cites: 3,657,699; 3,250,855; 3,170,033; 3,038,028.)

* 79. Horst Feistel, "Block cipher cryptographic system," U.S. Pat. No. 3,798,359., Field 178-22, Mar. 19, 1974, Ass. to IBM, (Cites: 3,657,699; 2,984,700; 3,170,033; 2,995,624; 2,917,579.)

* 80. Horst Feistel, "Step code ciphering system," U.S. Pat. No. 3,798,360., Field 178-22, Mar. 19, 1974, Ass. to IBM, (Cites: 3,522,374.)

81. Kurt Ehrat, "Method and apparatus for encoding and decoding messages," U.S. Pat. No. 3,808,365., Field 178-22, Apr. 30, 1974, (Cites: 3,614,316; 3,427,399; 3,170,033.)

82. John Spackman Reynolds, "Communication scrambler system," U.S. Pat. No. 3,808,536., Field 178-22, Apr. 30, 1974, Ass. to General Electric, (Cites: 3,696,207; 3,659,046; 3,614,316; 3,560,659; 3,123,672.)

83. Patrick A. Hughes, et. al., "Secure data transmission apparatus," U.S. Pat. No. 3,813,493., Field 178-22, May 28, 1974, (Cites: 3,711,645; 3,651,261; 3,427,399; 3,384,705; 3,341,659; 3,291,908.)

84. Richard Charles French, "Privacy transmission system," U.S. Pat. No. 3,824,467., Field 178-22, July 16, 1974, Ass. to Philips Corp., (Cites: 3,731,197; 3,657,699; 3,188,391; 3,105,114; 2,453,659.)

85. Barrie O. Morgan, Kenneth M. Branscome, George E. Goode and John Q. Atchley, "Digital cryptographic system and method," U.S. Pat. No. 3,876,832., Field 178-22, Apr. 8, 1975, Ass. to Datotek, (Cites: 3,749,832; 3,546,380; 3,496,291; 3,480,915; 2,874,215; 2,406,829; 2,406,023.)

86. Barrie O. Morgan, et. al., "Digital cryptographic system and method," U.S. Pat. No. 3,878,331., Field 178-22, Apr. 15, 1975, Ass. to Datotek, (Cites: 3,740,475; 3,670,104; 3,502,793; 3,349,175; 3,057,955; 2,874,215; 2,401,454.)

87. Barrie O. Morgan, et. al., "Digital cryptographic system and method," U.S. Pat. No. 3,878,332., Field 178-22, Apr. 15, 1975, Ass. to Datotek, (Cites: 3,678,198; 3,670,104; 3,651,261; 3,546,380; 3,502,793; 3,291,908; 3,057,955; 2,874,215.)

* 88. Douglas J. Bartek and Thomas H. Howell, "Nonlinear code generator and decoder for transmitting data securely," U.S. Pat. No. 3,911,216., Field 178-22 Oct. 7, 1975, Ass. to Honeywell Info. Syst., (Cites: 3,838,259; 3,796,830; 3,784,743; 3,761,696; 3,711,645; 3,700,806; 3,691,472; 3,614,316; 3,515,805; 3,421,146.)

* 89. Thomas Mann Dennis, "Combined scrambler encoder for multilevel digital data," U.S. Pat. No. 3,925,611., Field 178-22, Dec. 9, 1975, Ass. to Bell Telephone Labs, (Cites: 3,829,779; 3,784,743; 3,753,113; 3,649,915.)

90. Gustav Guanella, et. al., "Digital scrambling apparatus for use in pulsed signal transmission," U.S. Pat. No. 3,925,612., Field 178-22, Dec. 9, 1975, (Cites: 3,093,796; 3,069,657.)

* 91. Danforth K. Gannett, "Key generating system," U.S. Pat. No. 3,934,078., Field 178-22, Jan. 20, 1976, Ass. to Bell Telephone Labs, (Cites: 2,466,044; 2,429,471; 2,428,149; 2,424,999; 2,424,998; 2,406,977; 2,395,467; 2,289,564; 2,284,401.)

* 92. Carl Obeginski, "Method and apparatus for altering the synchronous compare character in a digital date communication system," U.S. Pat. No. 3,936,601., Field 178-22, Feb. 3, 1976, Ass. to Burroughs Corp., (Cites: 3,598,914; 3,546,384; 3,532,985; 3,472,956.)

* 93. W.F. Ehrsam, "Block cipher system for data security," U.S. Pat. No. 3,958,081., Field 178-22, May 18, 1976, Ass. to IBM, (Cites: 3,798,360; 3,798,359.)

* 94. Kurt Ehrat, "Method and apparatus for transmitting and receiving electrical speech signals transmitted in ciphered or coded form," U.S. Pat. No. 3,959,592., Field 179-1.5E, May 25, 1976, (Cites: 3,504,286; 2,672,512; 2,640,880; 2,627,541.)

* 95. W.F. Ehrsam, "Product block cipher system for data security," U.S. Pat. No. 3,962,539., Field 178-22, June 8, 1976, Ass. to IBM, (Cites: 3,798,360; 3,798,359.)

96. Gustav Guanella, "Method and device for the coded transmission of messages," U.S. Pat. No. 3,970,790., Field 178-22, July 20, 1976, (Cites: 3,824,467; 3,796,830; 3,731,197; 3,657,699; 3,188,391.)

97. Ralph L. Miller, "Telephone privacy system," U.S. Pat. No. 3,976,839., Field 178-22, Aug. 24, 1976, Ass. to Bell Telephone Labs, (Cites: 2,429,608; 2,366,583.)

98. Markus Bruckner, Gustav Guanella, et. al., "Method and apparatus for the secret transmission of speech," U.S. Pat. No. 3,978,288., Field 179-1.5R, Aug. 31, 1976. (Cites: 3,399,273; 2,932,693; 2,405,599; 2,107,756.)

99. Eugene Peterson, "Signaling system," U.S. Pat. No. 3,979,558., Field 179-1.5R, Sept. 7, 1976, Ass. to Bell Telephone Laboratories, (Cites: 2,411,683; 2,151,091; 2,132,205; 1,752,485.)

* 100. Danforth K. Gannett, "Key pulse generator for secrecy signaling circuit," U.S. Pat. No. 3,983,326., Field 178-22, Sept. 28, 1976, Ass. to Bell Telephone Labs., (Cites: 2,236,705; 2,145,332; 2,089,639; 1,965,121; 1,954,170.)

101. Homer W. Dudley, "Secret telephony," U.S. Pat. No. 3,985,958., Field 179-1.5R, Oct. 12, 1976, Ass. to Bell Telephone Labs, (Cites: 2,395,431; 2,107,756; 2,098,956.)

* 102. Michael David Patten, "Digital data scrambler and descrambler," U.S. Pat. No. 3,988,538., Field 178-22, Oct. 26, 1976, Ass. to International Standard Electric Corp., (Cites: 3,784,743; 3,649,915; 3,515,805; 3,452,328.)

* 103. Kenneth M. Branscome, et. al., "Voice security method and system," U.S. Pat. No. 3,991,271., Field 178-22, Nov. 9, 1976, Ass. to Datotek, (Cites: 3,773,977; 3,586,776; 3,463,911; 2,411,683.)

* 104. Takashi Araseki, et. al., "Speech signal presence detector," U.S. Pat. No. 4,001,505., Field 179-1.5R, Jan. 4, 1977, Ass. to Nippon Electric, (Cites: 3,507,999; 3,488,446; 3,278,685.)

* 105. Harold S. Richard, et. al., "Programmable cryptic device for enciphering and deciphering data," U.S. Pat. No. 4,004,089., Field 178-22, Jan. 18, 1977, Ass. to NCR Corp., (Cites: 3,911,216; 3,824,467; 3,798,360; 3,798,359; 3,781,473; 3,773,977; 3,731,197; 3,657,699; 3,522,374.)

* 106. Kenneth M. Branscome, "Voice security method and system," U.S. Pat. No. 4,013,837., Field 178-22, Mar. 22, 1977, Ass. to Datotek, (Cites: 3,777,133; 3,760,355; 3,725,689; 3,723,878; 3,694,757; 3,598,979; 3,463,911; 3,167,738.)

107. Kenneth M. Branscome, et. al., "Voice security method and system," U.S. Pat. No. 4,020,285., Field 179-1.5R, Apr. 26, 1977, Ass. to Datotek, (Cites: 3,921,151; 3,909,534; 3,824,467; 3,773,977; 2,586,475.)

* 108. Robert R. Willmore, "Apparatus for the identification of feedback tapes in a shift register generator," U.S. Pat. No. 4,034,156., Field 178-22, July 5, 1977, Ass. to U.S. Govt., Secy of Air Force, (Cites: 3,670,151; 3,599,209; 3,598,979; 3,439,279; 3,217,297.)

109. Denmer Dix Baxter, "Walsh function signal scrambler," U.S. Pat. No. 4,052,565., Field 178-22, Oct. 4, 1977, Ass. to Martin Marietta Corp., (Cites: 3,859,515; 3,742,201; 3,678,204; 3,204,035.)

* 110. A.A. Jorgensen, "All digital delta to PCM converter," U.S. Pat. No. 4,057,797., Field 340-347DD, Nov. 8, 1977, Ass. to Stromberg Carlson.

111. S.T.K. Johansson, "Arrangement for ciphering and deciphering of information," U.S. Pat. No. 4,058,673., Field 178-22, Nov. 15, 1977.

112. Peter Maitland, et. al., "Sound scrambling equipment," U.S. Pat. No. 4,058,677., Field 179-1.5R, Nov. 15, 1977, Ass. to Lear Siegler Inc., (Cites: 3,696,207; 3,155,908; 2,510,338; 2,509,716; 2,411,206.)

* 113. Jean-Pierre Adoul, "Method and apparatus for speech detection of PCM multiplexed voice channels," U.S. Pat. No. 4,061,878., Field 179-1.5R, Dec. 6, 1977, Ass. to Universite de Sherbrooke, Canada, (Cites: 3,985,956; 3,878,337.)

* 114. R.E. Malm, "Vocoder systems providing waveform analysis and synthesis using Fourier Transform representation of signal," U.S. Pat. No. 4,064,363., Field 179-1SA, Dec. 20, 1977, Ass. to Northrop Corp., (Cites: 3,026, 375; 3,344,349; 3,360,610; 3,403,227; 3,471,648.)

115. M.V. Franssen, "Signal transmission circuit comprising a coder and decoder," U.S. Pat. No. 4,064,505., Field 340-347DD, Dec. 20, 1977, Ass. to U.S. Philips Corp., (Cites: 3,225,142; 3,631,232.)

116. Y. Saeki and H. Udmera, "Video scrambler and descrambler apparatus," U.S. Pat. No. 4,064,536., Field 358-118, Dec. 20, 1977, Ass. to Pioneer Electronic Corp., (Cites: 3,081,376; 3,729,576; 3,936,593.)

117. L.L. Goldberg, "Check digit generation and verification apparatus," U.S. Pat. No. 4,065,752., Field 340-146.1AJ, Dec. 27, 1977, (Cites: 3,384,902; 3,544,776.)

* 118. R.P. Ridings, Jr. and R.H. Lanter, "Adaptable zero order predictor for speech predictive encoding communications systems," U.S. Pat. No. 4,066,844., Field 179-15BW, Jan. 3, 1978, Ass. to Communication Satellite Corp., (Cites: 3,584,145; 3,588,364; 3,689,698; 3,711,650; 3,927,268.)

119. Pierre Schmid, et. al., "Method and apparatus for the scrambled transmission of spoken information via a telephony channel," U.S. Pat. No. 4,068,094., Field 179-1.5R, Jan. 10, 1978, (Cites: 3,688,193; 3,201,517; 3,133,991; 3,012,098; 2,411,206; 1,921,063; 1,819,614.)

* 120. H.V. Shutterly, "Secure television transmission system," U.S. Pat. No. 4,070,693., Field 358-123, Jan. 24, 1978, Ass. to Westinghouse Electric Corp., (Cites: 3,746,799; 3,821,731; 3,830,966; 3,919,462; 3,921,151; 3,925,611; 3,958,081.)

* 121. J.E. Roberts and R.H. Wiggans, "Piecewise linear predictive coding system," U.S. Pat. No. 4,070,709., Field 364-602, Jan. 24, 1978, Ass. to U.S. Govt, Secy. of Air Force, (Cites: 3,502,986; 3,740,476; 3,927,268; 3,973,081; 3,973,199.)

122. R.H. Miller, W. Dyer, J.A. Winterbury, W.A. Carlson and R.O. Eastman, "Quantized non-synchronous clipped speech multi-channel coded communications system," U.S. Pat. No. 4,071,705., Field 179-15BA, Jan. 31, 1978, Ass. to U.S. Govt., Secy. of Navy, (Cites: 2,902,542; 2,962,553.)

* 123. W.G. McGussin, "Adaptive delta modulation system," U.S. Pat. No. 4,071,825., Field 325-38B, Jan. 31, 1978, Ass. to RCA Corp., (Cites: 3,609,551; 3,699,566; 3,727,135; 3,857,111; 3,922,606; 3,995,218.)

* 124. Y. Tokura and S. Hashimoto, "Method and apparatus for judging voiced and unvoiced condition of a speech signal," U.S. Pat. No. 4,074,069., Field 179-1SC, Feb. 14, 1978, Ass. to Nippon Telegraph and Telephone Public Corp., (Cites: 3,662,115; 3,740,476.)

125. B.L. Jansen, "Telephone privacy device," U.S. Pat. No. 4,074,078., Field 179-84C, Feb. 14, 1978, Ass. to Rainen Lee Organization Inc., (Cites: 3,061,783; 3,187,108; 3,226,489; 3,293,371; 3,514,548; 3,515,806; 3,614,326; 3,654,396; 3,784,721; 3,793,487; 3,859,462.)

126. J.L. Tanner and B.A. Rist, "Television security system," U.S. Pat. No. 4,074,311., Field 358-118, Feb. 14, 1978, Ass. to Tanner Electronic Systems, (Cites: 2,905,747; 3,202,758; 3,347,982; 3,760,097; 3,896,262.)

7.3 ALPHABETICAL LIST OF PATENTEE'S OF RELATED U.S. PATENTS

1. Adoul, Jean-Pierre: 4,061,878.
2. Aiken, Howard H.: 3,657,476.
3. Alexanderson, E.F.W.: 1,426,944.
4. Andrews, D.E., Jr.: 3,614,316.
5. Angeleri, Emanuele: 3,659,046.
6. Araseki, Takashi: 4,001,505.
7. Atchley, John Q.: 3,876,832; 3,878,331; 3,878,332.
8. Bartek, Douglas J.: 3,911,216.
9. Baxter, Denmer Dix: 4,052,565.
10. Belin, E.: 1,657,366.
11. Bellamy, J.I.: 1,953,918.
12. Bemis, E.W.: 2,401,454.
13. Black, H.S.: 3,020,350.
14. Blackwell, O.B.: 1,598,673.
15. Branscome, Kenneth M.: 3,991,271; 4,013,837; 3,876,832; 3,878,331; 3,878,332; 4,020,285.
16. Branson, David E.: 1,470,594.
17. Braun, William V.: 3,639,690.
18. Briggs, L.A.: 2,401,855.
19. Broertjes, W.: 1,869,659.
20. Bruckner, Markus: 3,978,288.
21. Carlson, W.A.: 4,071,705.
22. Carpe, A.: 1,676,321.
23. Cartier, Francoise: 1,878,967.
24. Crimmins, James W.: 3,775,562.
25. Cronburg, C.I.: 2,403,888.
26. Cummings, G.C.: 1,352,116.
27. Czegho, C.S.: 2,401,985.
28. Damm, A.G.: 1,502,376; 1,715,904.
29. Dennis, Thomas Mann: 3,925,611.
30. Dudley, Homer W.: 3,985,958.
31. Dyer, W.: 4,071,705.
32. Eastman, R.O.: 4,071,705.
33. Eaves, A.J.: 1,356,701.
34. Ehrat, Kurt: 3,678,198; 3,808,365; 3,959,592.
35. Ehrsam, W.F.: 3,958,081; 3,962,539.
36. Feistel, Horst: 3,798,359; 3,798,360.
37. Franssen, M.V.: 4,064,505.
38. French, Richard Charles: 3,824,467.
39. Friedman, W.F.: 1,516,180; 2,139,676.
40. Gammell, E.O.: 2,401,474; 2,401,475.
41. Gannett, Danforth K.: 3,934,078; 3,983,326.
42. Gentges, Frank H.: 3,746,799.
43. Goldberg, L.L.: 4,065,752.
44. Goodall, W.M.: 3,071,649.
45. Goode, George E.: 3,781,472; 3,781,473; 3,876,832; 3,878,331; 3,878,332.

46. Greene, M.L.: 2,401,477.
47. Guanella, Gustav: 3,651,261; 3,925,612; 3,970,790; 3,978,288; 3,536,833.
48. Hagelin, B.C.W.: 2,394,765.
49. Hagersten, B.F.: 3,557,307.
50. Hammond, J.H., Jr.: 1,910,540.
51. Harper, A.U.: 1,529,786.
52. Hartley, R.V.L.: 1,605,023.
53. Hashimoto, S.: 4,074,069.
54. Hetlevik, C.S.: 3,602,645.
55. Hicks, R.M.: 2,403,280.
56. Hitt, Parker: 1,848,291.
57. Howell, Thomas H.: 3,911,216.
58. Hughes, Patrick A.: 3,813,493.
59. Jansen, B.L.: 4,072,078.
60. Jipp, A.: 1,912,983.
61. Johansson, S.T.K.: 4,058,673.
62. Johnson A.F. and Johnson B.F.: 253,061.
63. Jorgensen, A.A.: 4,057,797.
64. Korn, W.: 1,733,886.
65. Lanter, R.H.: 4,066,844.
66. Lindner, H.G.: 3,025,350.
67. Maitland, Peter: 4,058,677.
68. Malm, R.E.: 4,064,363.
69. Martin, W.B.: 2,401,494.
70. Mathes, R.E.: 2,175,847; 2,401,877.
71. McDonald, James A.: 3,688,193.
72. McGussin, W.G.: 4,071,825.
73. Miller, R.H.: 4,071,705.
74. Miller, Ralph L.: 3,976,839.
75. Molins, A.R.: 1,505,055.
76. Morehouse, L.F.: 1,356,546; 1,568,991.
77. Morgan, Barrie O.: 3,686,631; 3,876,832; 3,878,331; 3,878,332.
78. Nyberg, Sture: 3,683,513.
79. Obeginski, Carl: 3,936,601.
80. Parker, R.D.: 1,320,908; 1,442,819.
81. Patten, Michael David: 3,988,538.
82. Perry, D.B.: 2,265,120.
83. Peterson, Eugene: 3,979,558.
84. Pfannenstiehl, Harry: 1,491,358.
85. Pierce, R.E.: 1,312,574; 2,401,507.
86. Potts, L.M.: 1,558,280.
87. Ranger, R.H.: 1,794,389.
88. Reynolds, John Spackman: 3,808,536.
89. Richard, Harold S.: 4,004,089.
90. Ridings, R.P., Jr.: 4,066,844.
91. Rist, B.A.: 4,074,311.
92. Roberts, J.E.: 4,070,709.
93. Saeki, Y.: 4,064,536.
94. Schmid, Pierre: 4,068,094.

95. Schroeder, H.C.: 3,784,743.
96. Schroeder, M.R.: 3,328,526.
97. Shutterly, H.V.: 4,070,693.
98. Smart, J.H.: 1,900,772.
99. Smith, John Lynn: 3,796,830.
100. Spencer, J.A.: 2,397,057; 2,397,058.
101. Tanner, J.L.: 4,074,311.
102. Tokura, Y.: 4,074,069.
103. Udmera, H.: 4,064,536.
104. Vasseur, Jean-Pierre: 3,700,806.
105. Vernam, G.S.: 1,416,765; 1,479,846; 1,555,042; 1,686,585.
106. Walker, J.B.: 2,151,452.
107. Wiggans, R.H.: 4,070,709.
108. Willmore, Robert R.: 4,034,156.
109. Winterbury, J.A.: 4,071,705.
110. Wolper, Donald F.: 3,627,928.
111. Woodhead, Robert C.: 3,603,734.
112. Wrede, Franz: 1,945,014.

7.4 ALPHABETICAL LIST OF MAJOR ASSIGNEE'S OF RELATED U.S. PATENTS

1. American Telegraph and Telephone (A.T. and T.):
   1,320,908; 1,356,546; 1,416,765; 1,442,819; 1,479,846; 1,470,594; 1,529,786; 1,558,280; 1,568,991; 1,598,673; 1,555,042; 1,676,321; 1,686,585; 2,265,120; 2,401,454; 2,401,474; 2,401,475; 2,401,477; 2,401,494; 2,401,507; 2,403,888.

   Total 21 patents.

2. Associated Electric Laboratories:
   1,953,918.

   Total 1 patent.

3. Bell Telephone Laboratories:
   3,784,743; 3,925,611; 3,934,078; 3,976,839; 3,983,326; 3,979,558; 3,985,958; 3,020,350; 3,071,649; 3,328,526.

   Total 10 patents.

4. Burroughs Corporation:
   3,936,601.

   Total 1 patent.

5. Canadian Government:
   3,603,734.

   Total 1 patent.

6. Datotek:
   3,781,472; 3,781,473; 3,686,631; 3,991,271; 4,013,837; 3,876,832; 3,878,331; 3,878,332; 3,991,271; 4,020,285.

   Total 10 patents.

7. Data Transmission Sciences Inc.:
   3,775,562.

   Total 1 patent.

8. General Electric:
1,426,944; 3,808,536.

Total 2 patents.

9. Honeywell Information Systems:
3,911,216.

Total 1 patent.

10. International Business Machines (IBM):
3,796,830; 3,958,081; 3,962,539; 3,798,359; 3,798,360.

Total 5 patents.

11. International Communications Laboratories:
1,848,291.

Total 1 patent.

12. International Standard Electric Corp.:
3,988,538.

Total 1 patent.

13. Lear Siegler Inc.:
4,058,677.

Total 1 patent.

14. Litton Systems:
3,627,928.

Total 1 patent.

15. Martin Marietta Corp.:
4,052,565.

Total 1 patent.

16. Motorola:
3,639,690; 3,688,193.

Total 2 patents.

17. NCR Corp.:
4,004,089.

Total 1 patent.

18. Nippon Electric:
4,001,505.

Total 1 patent.

19. Philips Corp.:
3,824,467.

Total 1 patent.

20. Rauland Corp. of Chicago:
2,401,985.

Total 1 patent.

21. RCA:
1,794,389; 2,175,847; 2,397,057; 2,397,058; 2,401,855; 2,401,877.

Total 6 patents.

22. Stromberg Carlson:
4,057,797.

Total 1 patent.

23. Teleregister Corporation:
2,403,280.

Total 1 patent.

24. U.S. Government, Secy of Air Force:
4,034,156.

U.S. Government, Secy of Army:
3,025,350.

U.S. Government, Secy of Navy:
2,139,676; 3,614,316; 3,507,980.

Total 5 patents.

25. Universite de Sherbrooke:
4,061,878.

Total 1 patent.

26. Western Electric:
1,352,116; 1,356,701; 1,491,358; 1,605,023.

Total 4 patents.