ANALOG ENCRYPTION AND TRANSMISSION OF ANALOG SIGNALS

Frank Chethik
Ford Aerospace & Communications Corporation
Western Development Laboratories Division
3939 Fabian Way
Palo Alto, California 94303

ABSTRACT

A method of encryption and transmission of analog signals is presented in which Pulse-Amplitude-Modulation, Frequency Modulation (PAM-FM) techniques are used. This method has the potential for increased capacity over bandwidth constrained channels with no loss of privacy when compared to the current practice of Pulse-Code-Modulation, Phase-Shift-Keying (PCM-PSK). The techniques are described, and quantitative comparative analyses are given. A fading channel scenario is developed in which the capacity of PAM-FM with analog encryption is shown to be twice that of PCM-PSK.

INTRODUCTION AND SUMMARY

The development of sensor systems and telemetry systems of various types over the last few years has been characterized by expanded use of digital encoding and transmission technology. Encryption for privacy is easily accomplished with bit-for-bit encryption incurring no error multiplication effects nor degradation in recovering the analog variables that are quantized and transmitted. Certain classes of systems, however, require the transmission of sizeable analog bandwidth signals perhaps on the order of 10’s or 100’s of megahertz, and encryption of these signal bandwidths requires one or several gigabits per second. Such systems are planned and in the works and are in various stages of development.

The constraints on transmission bandwidth, in many cases, limit the rate of analog information flow over the system. Thus, for channel-bandwidth limited systems, the pressure for relay of higher analog information rates (hereafter referred to as baseband signals) has motivated the reexamination of the encoding-transmission methodology. An alternative method of encoding transmission that exhibits more efficient use of transmission bandwidth under certain conditions is PAM-FM. Comparison with the current art PCM-PSK digital system yields the following conclusions. For output signal-to-noise ratios (SNRs) less than approximately 45 dB at the received baseband port, the PAM-FM technique is both more bandwidth efficient and transmission channel power efficient than PCM-PSK. Furthermore, for the transmission channels that require large power margin due to path fading, the PAM-FM technique can take advantage of the high SNR circumstance with either improved baseband SNR or increased baseband capacity.

DESCRIPTION OF THE ANALOG ENCRYPTION SYSTEM (AES) CONCEPT

The AES concept embodies two major processes: (1) *converting* between the clear text analog baseband signal and the cipher text analog signal, and (2) *transmitting* the cipher text analog signals. The analog transmission method is classical PAM and is chosen because the analog key generation and synchronization require coherent clocking. The PAM technique transmits analog variables as a sequential, time-discrete process in which PAM symbol timing is intrinsic to the waveforms, and the synchronous clock is recoverable at the destination.

Analog Encryption Algorithm

The basic method employs the cyclic addition of an analog key to time-discrete samples of the signal baseband. A multiplication of +1 or -1, an additional key variable occurring at the sample rate, provides an additional level of security as shown in Figure 1. The modulo-A_m adder operates in accordance with the rules shown in Table 1.

The decryption process performs the reversal of the multiplication/cyclic addition steps, The process is essentially nonambiguous except for some ambiguity about values of S_i that fall near $+A_m$ or $-A_m$. The modulo-A_m, subtractor operates according to the rule in Table 11.

Some waveforms that describe the encryption/decryption processes are shown in Figure 2. This is a simplified graphical representation to aid understanding of the processes.

Transmission System

PAM cipher stream transmission is accomplished by means of a frequency modulation system shown in Figure 3. Bandlimiting the PAM to create Nyquist shaped symbols is an important characteristic of the filtering and equalization processes required for suppression of intersymbol interference.

For much of the discussion in the next paragraph in which the PAM-FM system performance is compared with the currently popular PCM-PSK systems, it is assumed that the channel bandwidth is the major capacity-limiting constraint in the system. Thus, given a base bandwidth in the PAM-FM system, the FM modulation index is adjusted to cause the RF spectrum to nearly fully occupy the passband of the transmission channel. Given sufficient SNR to overcome the demodulator threshold requirements, the receiver signal quality is maximized by maintaining the largest supportable frequency deviation.

PERFORMANCE ANALYSIS

Encryption Performance

The performance of any encryption or privacy algorithm is dependent on two properties of the system: (1) the nonpredictability of the code or key with which the clear text is encoded, and (2) the method of combinatorial mapping of the clear text into the cipher test with the key. Criteria for judging the effectiveness of an encryption method may include issues such as immunity of the cipher text from code breaking as well as traffic analysis. It is expected that the statistical properties of the cipher text remain unchanged in the presence or absence of clear text and are unaltered by the specific nature of the clear text. Also the average cipher text spectrum properties must bear no relationship to nor be altered by that of the clear text. A game-theory simulation of the encryption process was performed in which the analog key was constructed by means of numerical operation on very long (nonperiodic over the experiment length) pseudonoise sequences. A baseband signal comprised of three sinusoids at mutually irrational frequencies were chosen to comprise the clear text baseband. Discrete Fourier transforms (DFTs) of the clear text signal, the enciphered signal, and the magnitude of the enciphered signal with and without the clear text signal are shown in Figures 4, 5, and 6. No frequency components of the baseband are evident, and the spectral density of the enciphered baseband appears uniform (white). No significant differences between the DFTs with or without input clear text were evident in the trials implying that the signal privacy and immunity from traffic analysis criteria have been satisfied.

Transmission System Performance

Since the mapping from the cipher system into the PAM clear text is single valued and (for the most part) linear, the root mean square (RMS) noise level that attends the demodulated PAM cipher symbols will also be present in the reconstituted clear text. Assuming that the RMS value of the clear text is the same as that of the cipher text PAM symbols, the analysis treats the PAM-FM signal as clear text signal. The comparison with the PCM-PSK is based on clear text PCM-PSK with no error multiplication effects.

PAM-FM Performance Analysis

An implementation of analog information transmission via a PAM-FM link is illustrated in Figure 7. The expected performance of this link is derived from the well known properties of frequency modulation, as described by Schwartz and others (1).

Sampling Frequency Considerations. The PAM sampling frequency, F_s, is assumed to be

$$F_s = 2.5 \text{ x } F_2 \qquad (1)$$

where F_2 is the highest baseband frequency of the baseband.

Pulse Shape Considerations. To minimize intersymbol interference in PAM, the signal pulse is designed to have a Nyquist pulse shape in the time domain and a cosine rolloff spectrum characteristic in the frequency domain as illustrated in Figure 8.

For this mode of transmission, the highest baseband frequency, F_2', that the PAM channel has to accommodate is

$$F_2{}^1 = \frac{F_s}{2}(1+\alpha) = \frac{2.5 \text{x} F_2 \text{x} 1.2}{2} = 1.5\, F_2 \quad \text{for } \alpha = 0.2 \qquad (2)$$

Signal Amplitude Distribution Considerations. For sine wave signal transmission, the signal is

$$S(t) = V \sin \omega t \qquad (3)$$

and the received signal power for a unity gain channel is

$$P_{sine} = \frac{1}{2} V^2 \qquad (4)$$

In the system illustrated in Figure 7, a Gaussian baseband truncated at 3σ is assumed.

The signal power with a Gaussian amplitude distribution is

$$P_G = \sigma^2 = (\frac{1}{3} V)^2 = \frac{1}{9} V^2 \qquad (5)$$

The receiver SNR penalty for a Gaussian signal relative to a sine wave signal is

$$\frac{SNR_G}{TTNR} = \frac{P_G}{P_{SINE}} = \frac{\frac{1}{9}V^2}{\frac{1}{2}V^2} = \frac{1}{4.5} = -6.5 \text{ dB} \qquad (6)$$

Performance Curves. After much arithmetic, the expected PAM-FM performance curves are derived. The expected baseband output signal-to-noise ratio is plotted in Figure 9 with $C/N_0\ F_2$ as the abscissa and in Figure 10 with $C/N_0,B_{IF}$ as the abscissa. In both figures the modulation index $\beta = \Delta F/F_2$ is a parameter ranging in value from 1.5 to 24. The optimum preemphasis/deemphasis improvement was estimated to be approximately 1 dB.

Data Clock Timing Recovery in PAM. Recovery of the data clock timing information from the demodulated baseband PAM analog signal has been discussed in references (2) and (3). Figure 11 taken from reference (2) illustrates the block diagram and the clock waveforms obtained in a PAM system. Jitter and bias errors are assumed to be reducible to arbitrarily small values.

PCM-PSK Performance Analysis. Digital transmission assumes sampling at 2.5 times the highest baseband signal frequency, quantization, and analog-to-digital conversion.

Quantization Noise. For a K-bit PCM word size there are 2K possible level values (N).

A dynamic range of ±V yields a quantization step size of

$$a = \frac{2V}{N} \tag{7}$$

A uniform baseband amplitude distribution over ±V yields an irreducible quantization noise

$$Q_n = \frac{a^2}{12} = \frac{V}{3N^2} \tag{8}$$

The output signal power is

$$S_o = \frac{a^2}{12}(M^2 - 1) = \frac{N^2 - 1}{N^2} \cdot \frac{V^2}{3} \tag{9}$$

and the output signal to quantization noise ratio is

$$\frac{S_o}{Q_n} = \frac{N^2 - 1}{N^2} \cdot \frac{V^2}{3} \cdot \frac{3N^2}{V^2} = N^2 - 1 \tag{10}$$

Bit Error Induced Noise. Due to the presence of thermal noise at the receiver input, some of the digital transmission errors will result in bit error induced noise power, (N_{BE}):

$$N_{BE} = \frac{a^2}{3}(2^{2k} - 1) \cdot P_e = \frac{4V^2}{3N^2}(N^2 - 1) \cdot P_e \tag{11}$$

where P_e is the probability of a bit error.

Effective Output Baseband Signal-to-Noise Ratio. Combining the quantization noise and the bit error induced noise on an RMS basis gives an effective output baseband signal-to-noise ratio which is

$$\mathrm{SNR} = \frac{\frac{N^2-1}{N^2} \cdot \frac{V^2}{3}}{\frac{V^2}{3N^2} + \frac{4V^2}{3N^2}(N^2-1) \cdot P_e} = \frac{N^2-1}{1 + 4P_e(N^2-1)} \tag{12}$$

The bit error induced noise will degrade the SNR by 3 dB when

$$1 + 4P_e(N^2-1) = 2 \tag{13}$$

and, therefore,

$$P_e = \frac{1}{4(N^2-1)} \tag{14}$$

A 1 dB degradation due to bit error induced noise will occur when

$$1 + 4P_e(N^2-1) = 1.259 \tag{15}$$

and, consequently,

$$P_e = \frac{0.259}{4(N^2-1)} \tag{16}$$

Performance Curves. With a quadriphase shift keying (QPSK) data link having a channel bandwidth corresponding to B . T_b = 1, i.e., -3 dB bandwidth at the first nulls of the QPSK spectrum, and allowing for a 2 dB BER performance degradation from an ideal channel, the expected baseband signal-to-noise ratio performance of the PCM transmission link is plotted in Figures 9 and 10 with $C/(N_0F_2)$ and $C/(N_0B_IF)$ on the abscissas, respectively. The word size k is a parameter of the family of curves.

An alternative form of graphic presentation of the results is given in Figure 12. Here, the throughput capacity normalized on IF bandpass is plotted parametric on the signal-to-noise ratio in the channel. Only a single line representation of the PCM-PSK system is needed because an increase in IF SNR above that required for digital transmission bit error rates (BERs) significantly below threshold produces no improvement in output SNR.

CONSIDERATIONS FOR SYSTEMS APPLICATIONS

New satellite systems requiring high capacity encrypted downlinks are forced to exploit the higher microwave bands (14 through 40 GHz). Depending on local climatic conditions and the radio path geometry, considerable path loss may be incurred, for example, as shown in Figure 13 which was compiled for the Washington, D.C. area (ref 4). The digital system must be designed with adequate margin to handle the statistically worst-case fade, because precipitous failure of the link would occur if SNRs below threshold were experienced. In contrast, the PAM-FM links can exploit the statistically likely excess link SNR by increasing baseband signal capacity and reducing FM deviation from those of the threshold conditions. Consider the following illustration.

Example Scenario

Assume that the required baseband SNR > 35 dB. The PCM system requires 6 bit word size yielding an allowable base bandwidth of 0.07 times the channel bandwidth. This operating condition is indicated as point A on Figure 14. The required input signal-to-noise ratio is about 12 dB. The same performance can be achieved with PAM-FM with a deviation ratio (β) of about 6, also yielding a baseband capacity of 0.07 of the channel passband. The channel SNR of 12 dB corresponding to point A may be the threshold condition which would be required to be met or exceeded for 99.8% of the time. Using the absorption statistics given in Figure 13 at 20 GHz, 5° elevation angle, it is observed that 98% of the time, the absorption is 5 dB or less. Thus 98% of the time, an additional 11 dB of channel SNR is available. However, no benefit to the PCM-PSK system results. The output SNR for the PAM-FM technique increases by 11 dB resulting in an output SNR of 46 dB. Alternatively, if more capacity is desired, a lower modulation index (β) is selected for a wider base-bandwidth so that the 35 dB output SNR is maintained. The base-bandwidth increases (as shown by operating point C on Figure 14) to about 0.13 of the channel passband, *nearly a 2-to-1 increase in capacity*.

This general capacity advantage is illustrated in Figure 15. In this figure, the capacity ratio between that of the PCM-PSK and the PAM-FM is given as a function of the required output SNR and available channel SNR. As evident in this figure, the capacity advantage of PAM-FM declines as the channel margins decline and as the output SNR requirement increases. At the required output SNR of 50 dB or more, the PCM-PSK system is more bandwidth efficient. For very low output SNRs, the upper bound for PCM-PSK capacity is 0.4 of the channel bandwidth. This derives from an assumed sample rate of 2.5 times the base-bandwidth and 1 bit encoding. The upper bound for the PAM-FM is also 0.4, assuming that Nyquist filtering of the PAM samples is taken at 2.5 times the base-bandwidth. The FM modulation index is assumed small enough when only the first order FM (PM) sidebands have significant power density. Thus, if the curves on Figure 12 and

14 were extended upward, they would all asymptote at a baseband capacity of 0.4 of the channel bandwidth.

CONCLUSIONS

As discussed in the preceding sections, there are certain situations when the implementation of the transmission link with a PAM-FM system is advantageous. In particular, when the operation is through a transmission medium that is subject to fading for short periods of time, the PAM-FM link will provide a large baseband signal-to-noise ratio most of the time dropping to threshold only during the fade. The PCM-PSK system, on the other hand, with its irreducible quantization noise will operate all the time close to its design threshold value.

In links experiencing predictable fades such as known weather conditions, the PAM-FM link can be operated most of the time with a capacity substantially larger than that of PCM-PSK link. The capacity of the PAM-FM link is reduced only during the duration of the fade to maintain the desired output signal quality. The PCM-PSK link, by comparison, cannot take advantage of this circumstance in a bandlimited channel.

ACKNOWLEDGMENT

The author acknowledges the major contributions of Mr. Leonard Lamin and Dr. Richard Sherman for their analysis and modeling efforts in evaluating the performance of the subject algorithm.

REFERENCES

1. Schwartz, M., *Information Transmission Modulation and Noise*. McGraw-Hill, 1959.

2. Franks, L.E. and J.P. Bubrouski, “Statistical Properties of Timing Jitter in PAM Timing Recovery Scheme,” *IEEE Transactions on Communications*, July, 1974.

3. Franks, L.E., “Carrier and Bit Synchronization in Data Communications,” *IEEE Transactions on Communications*, August, 1980.

4. Mitchell, W.C., “Rain Attenuation and Depolarization for the Washington, D.C. Area,” Technical Monograph, March, 1980, Ford Aerospace & Communications Corporation.

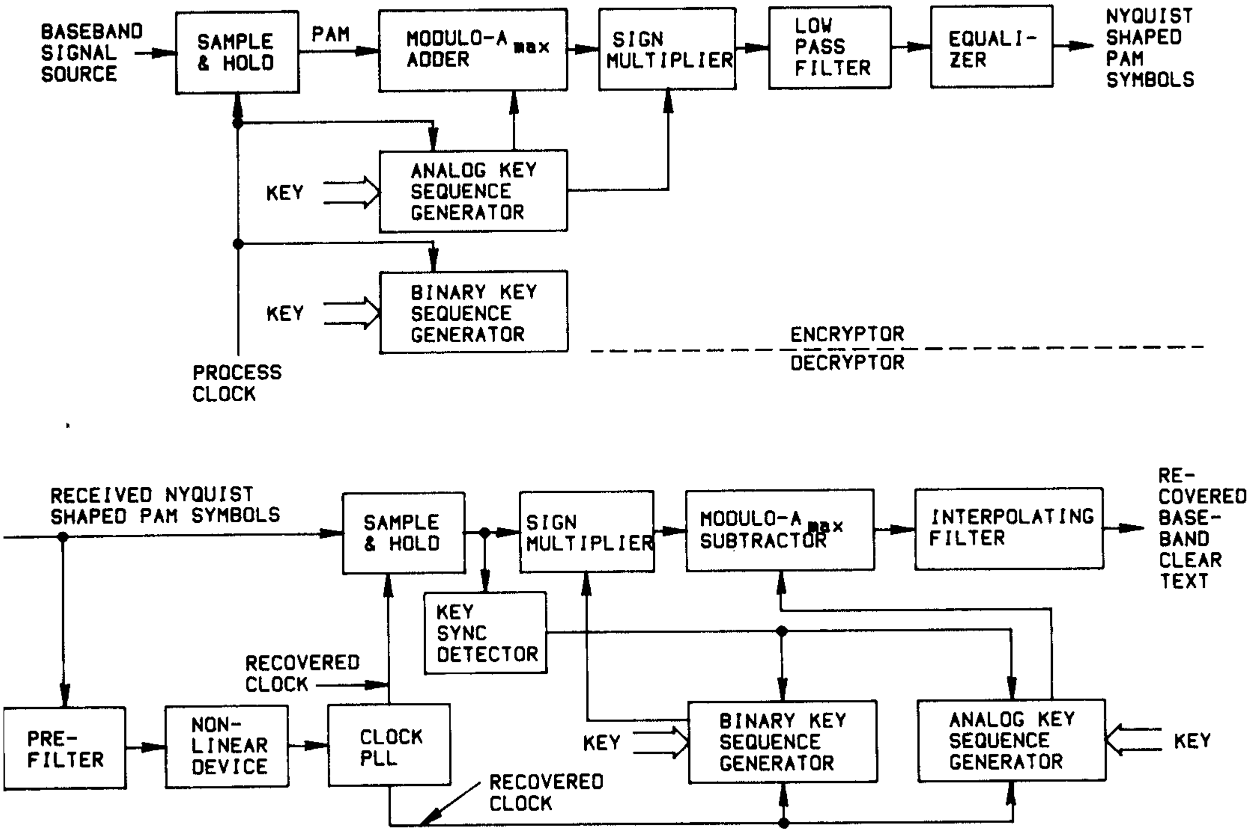


Figure 1 - AES Algorithm

TABLE I - Truth Table for Modulo-A_m Adder

$(S_i + K_i)$	C_i
$\|(S_i + K_i)\| < A_m$	$S_i + K_i$
$S_i + K_i > A_m$	$S_i + K_i - 2A_m$
$S_i + K_i < -A_m$	$S_i + K_i + 2A_m$

TABLE II -Truth TableforModulo-A_m Subtractor

$\hat{C}_i - K_i$	S_i
$\|\hat{C}_i - k_i\| < A_m$	$C_i - k_i$
$\hat{C}_i - k_i > A_m$	$C_i - k_i - 2A_m$
$\hat{C}_i - k_i < -A_m$	$C_i - k_i + 2A_m$

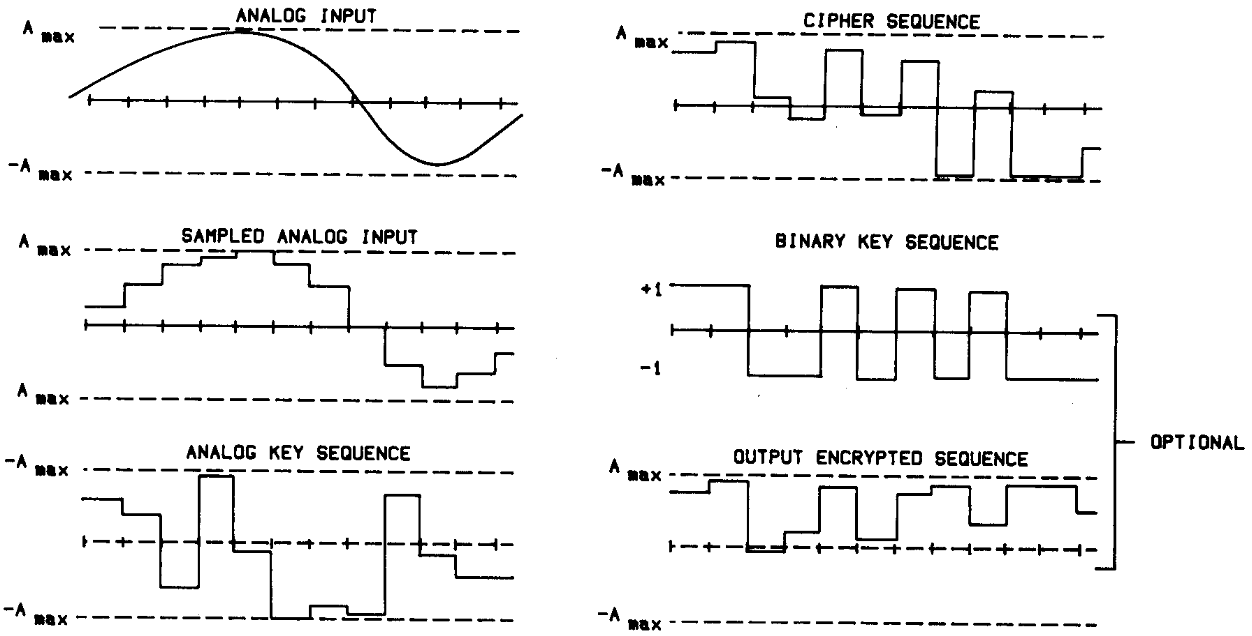


Figure 2 - Analog Encryption Process Waveforms

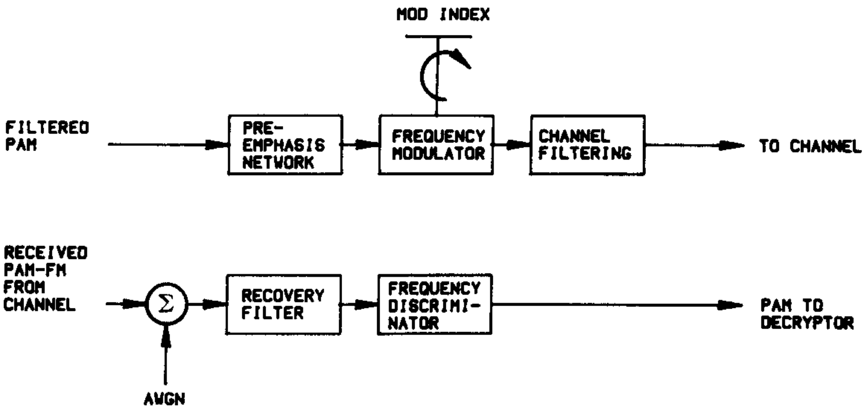


Figure 3 - FM Transmission System

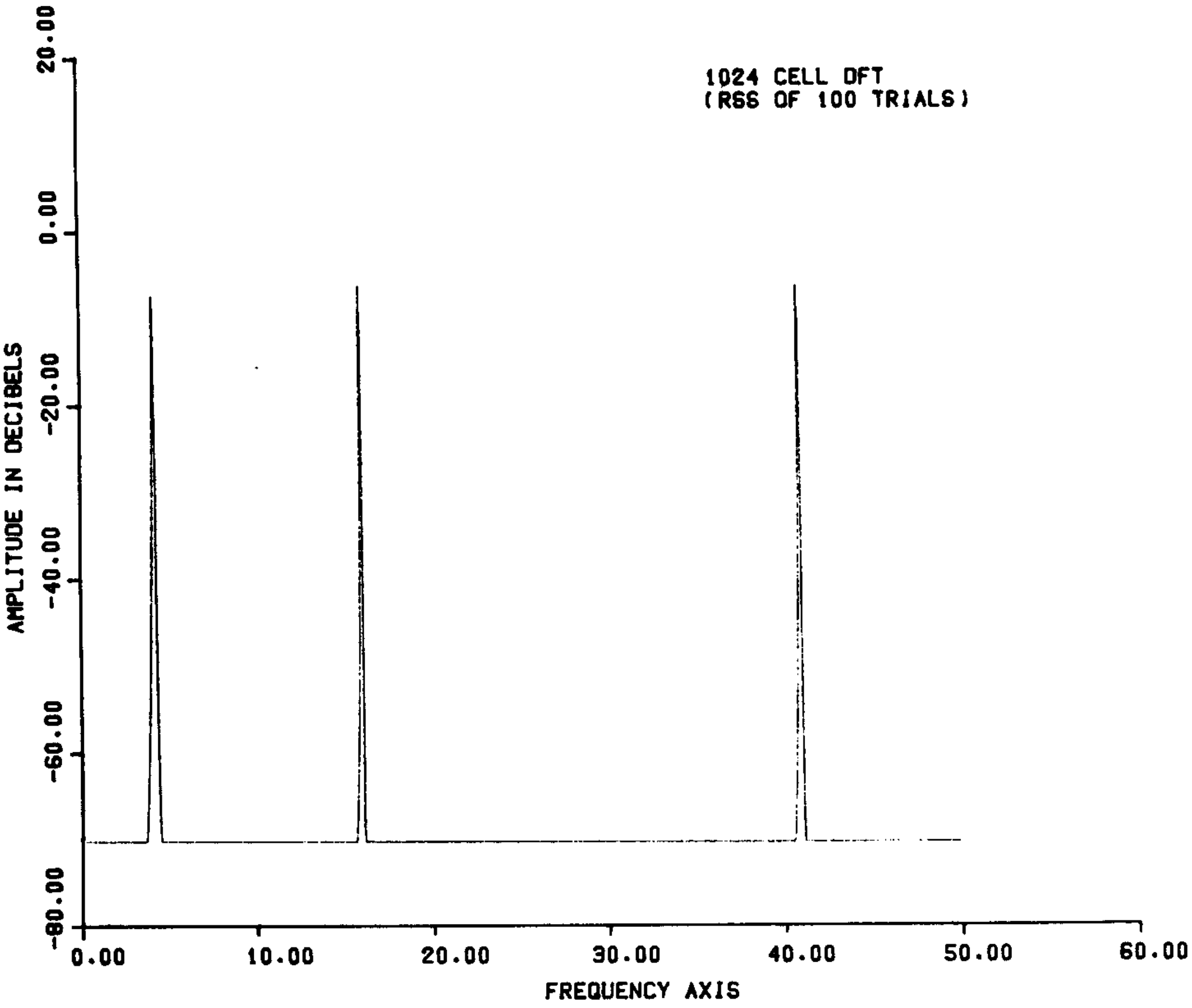


Figure 4 - Discrete Fourier Transform, Input Baseband Signal

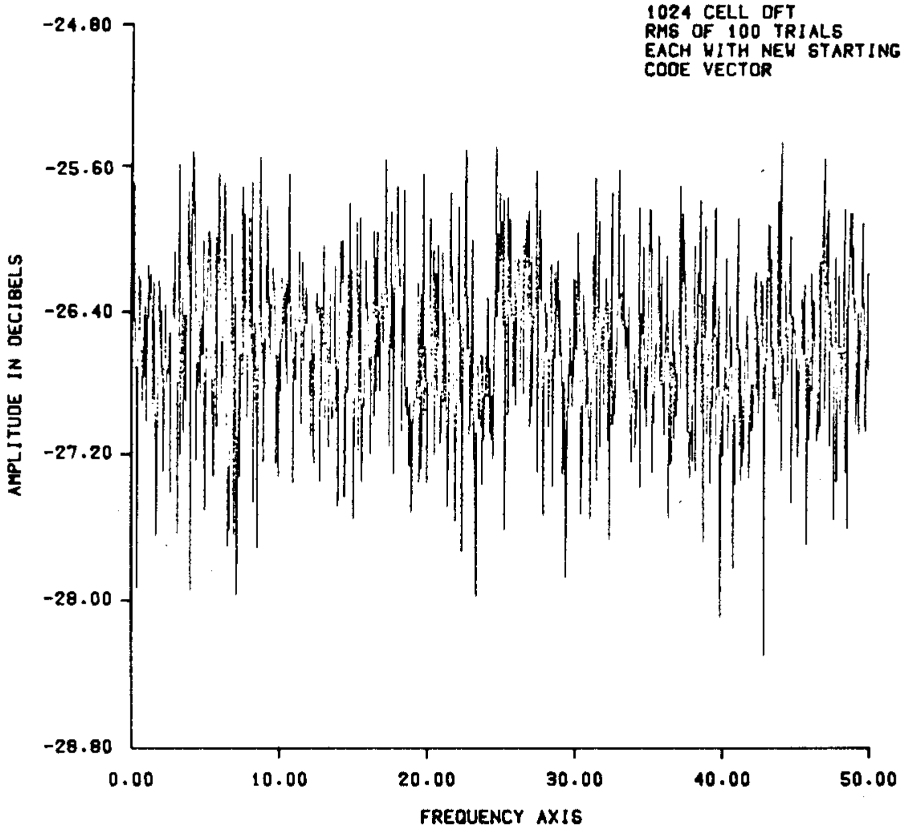


Figure 5a - Discrete Fourier Transform, PAM Encrypted Output Signal

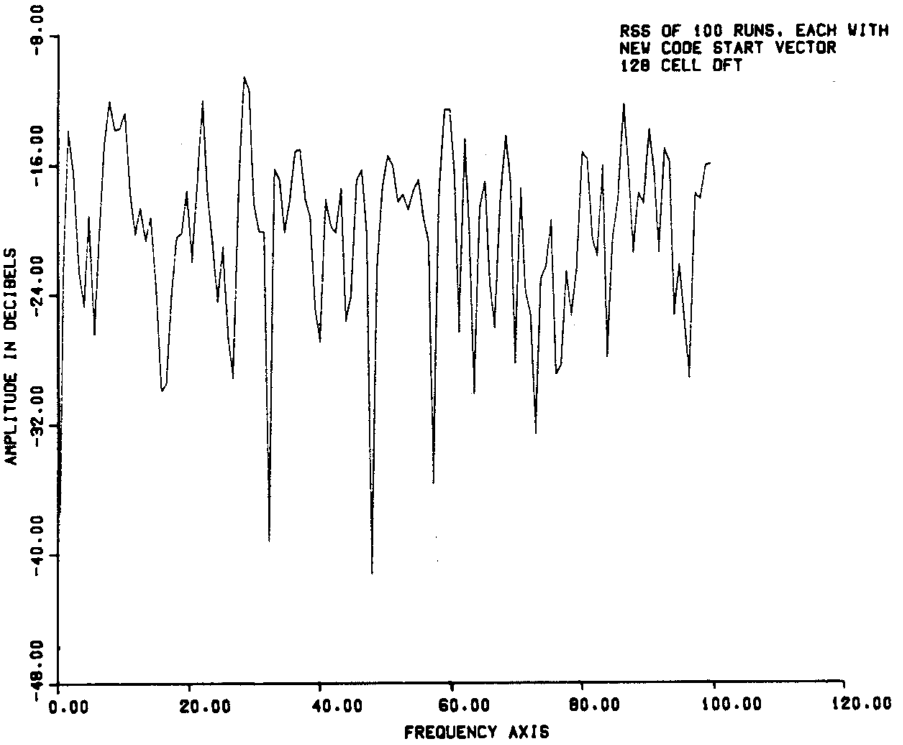


Figure 5b - Discrete Fourier Transform of Encrypted PAM Output Signal

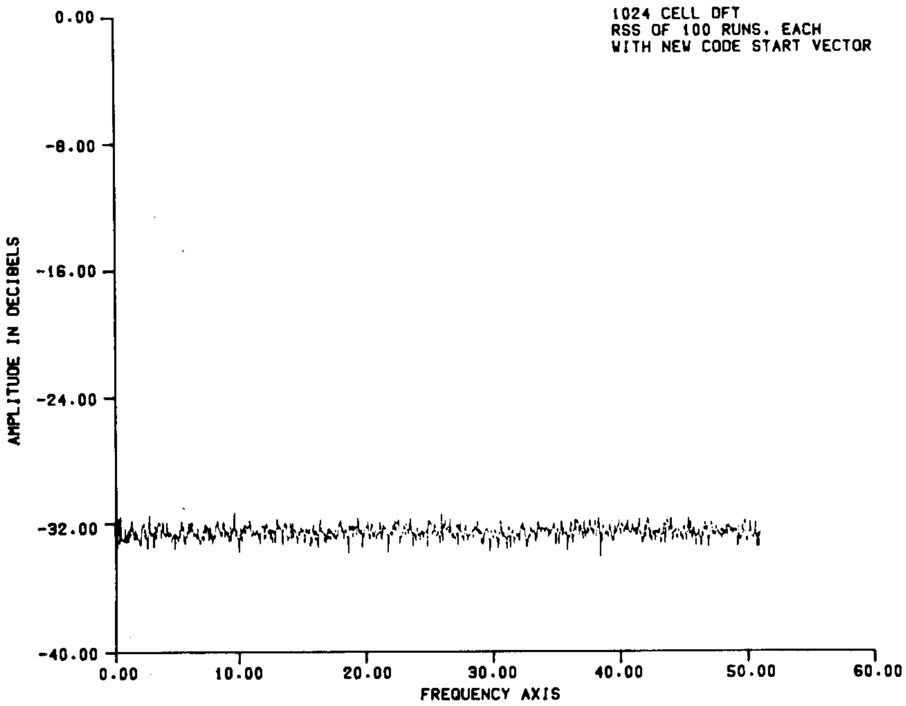


Figure 6 - Discrete Fourier Transform of Magnitude of Encrypted PAM Output Signal

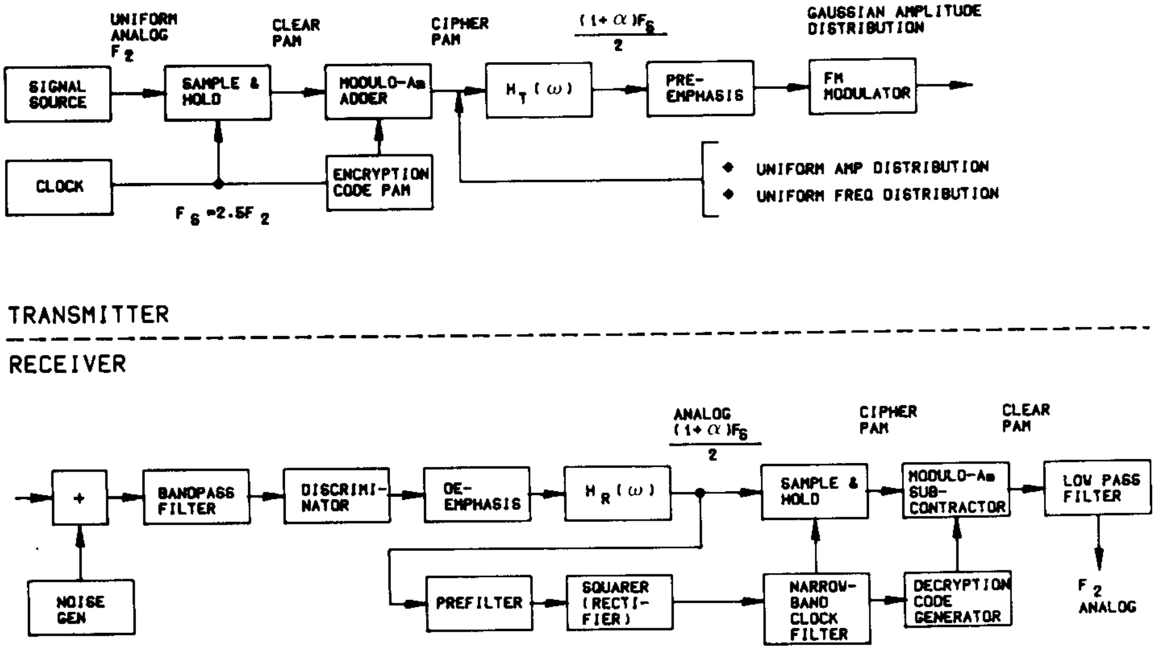


Figure 7 - Block Diagram of a PAM-FM Transmission System

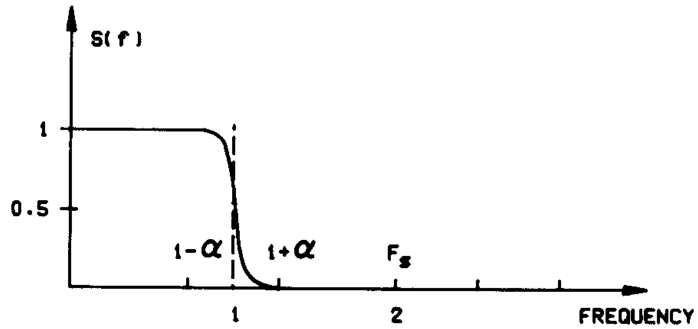


Figure 8 - Cosine Rolloff Spectrum

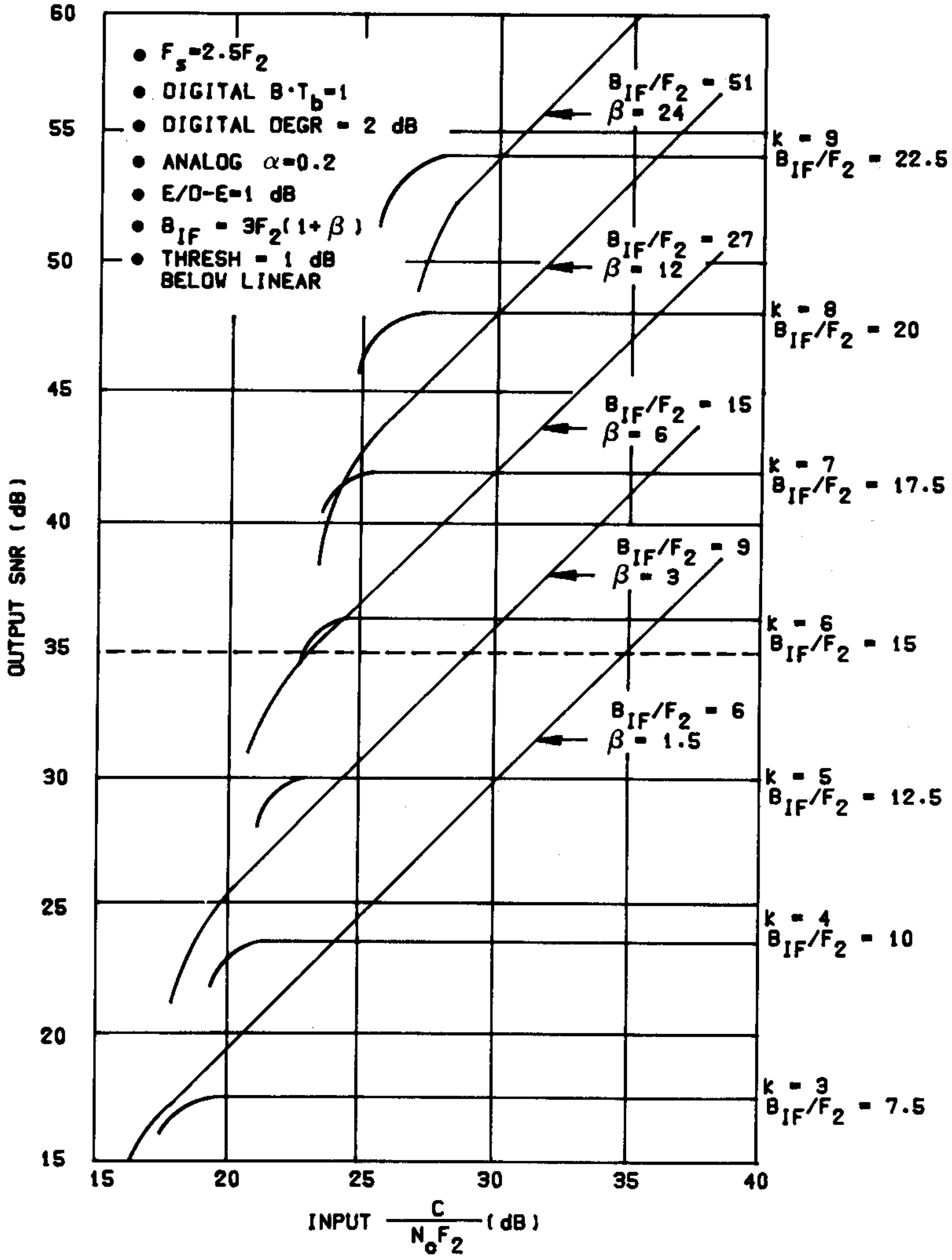


Figure 9 - Performance of PCM-PSK and PAM-FM Channels

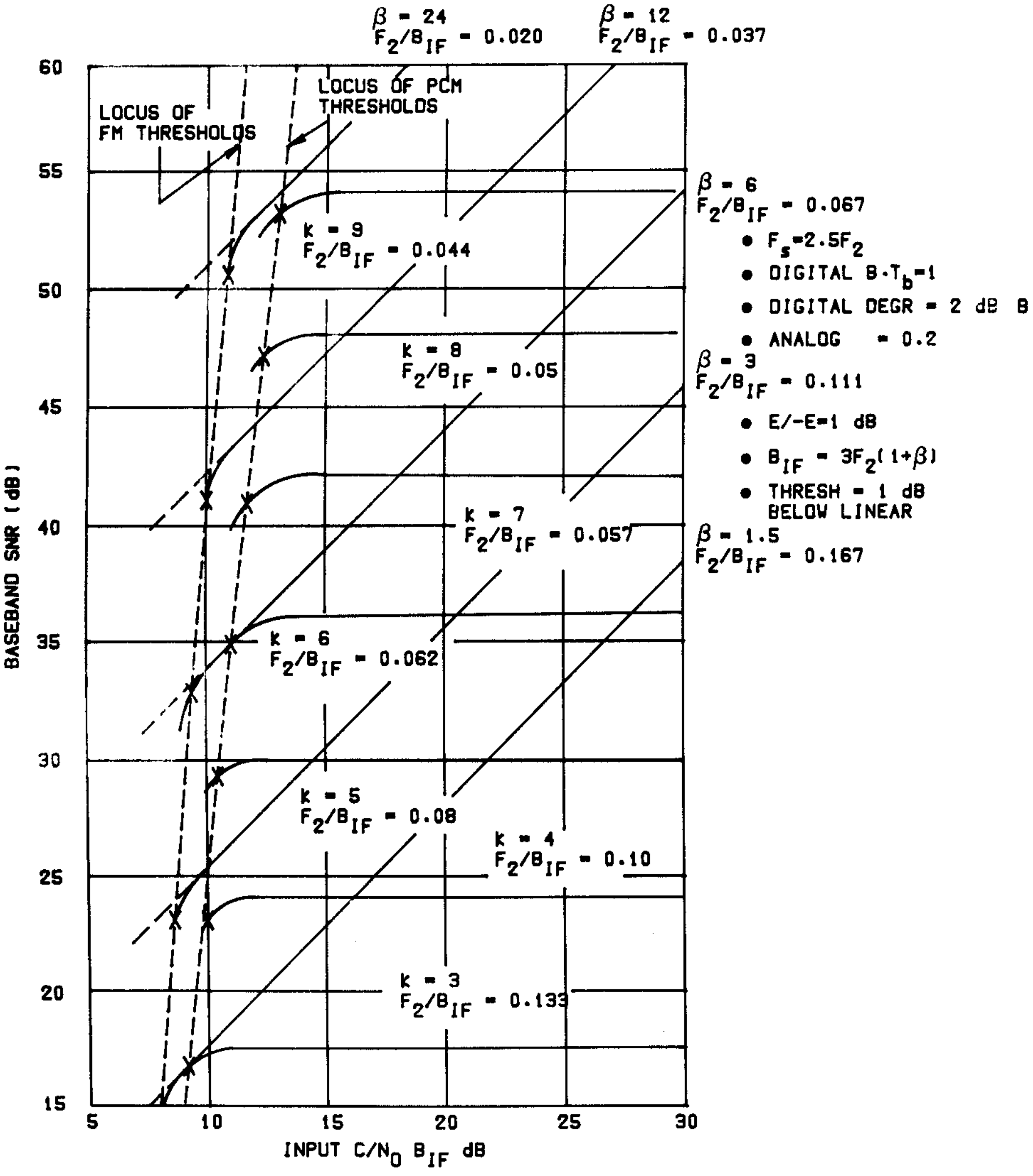
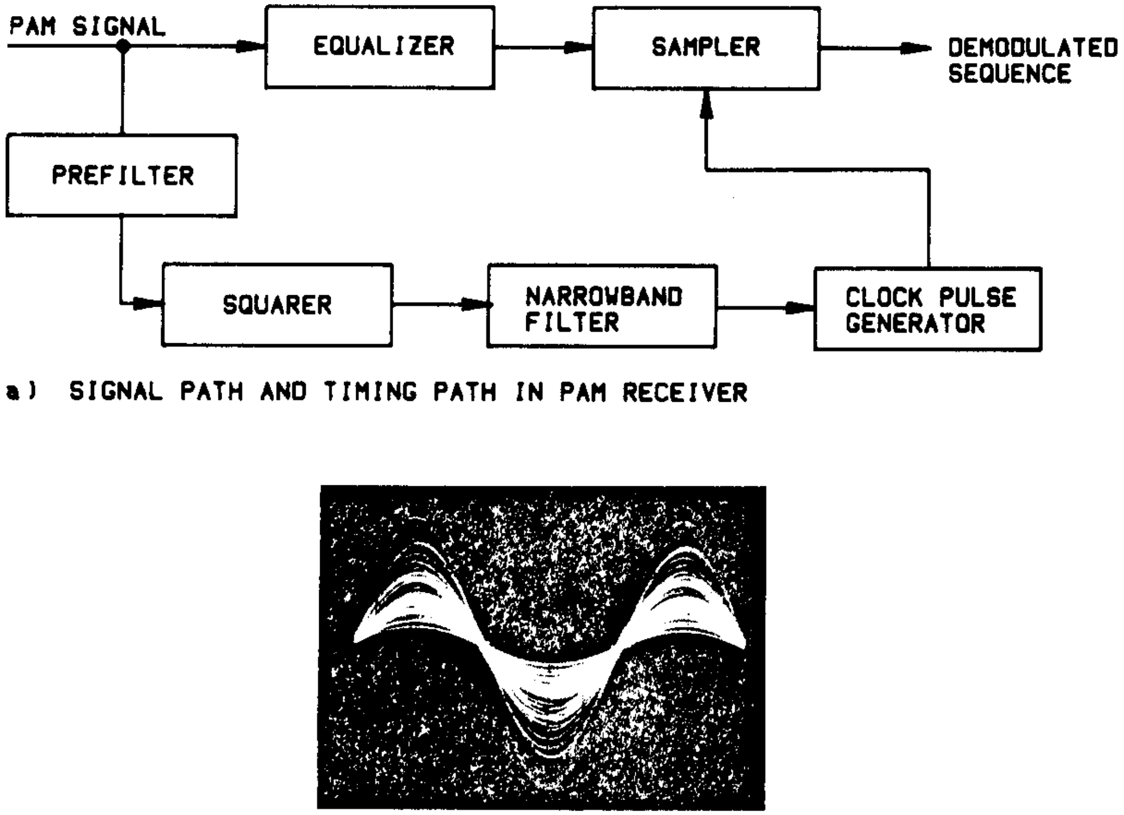


Figure 10 - Performance of PCM-PSK and PAM-FM Channels Normalized on Channel Bandwidth



a) SIGNAL PATH AND TIMING PATH IN PAM RECEIVER

b) OSCILLOGRAPHIC DISPLAY OF THE TIMING WAVE PROCESS

Figure 11 - Clock Timing Recovery in PAM

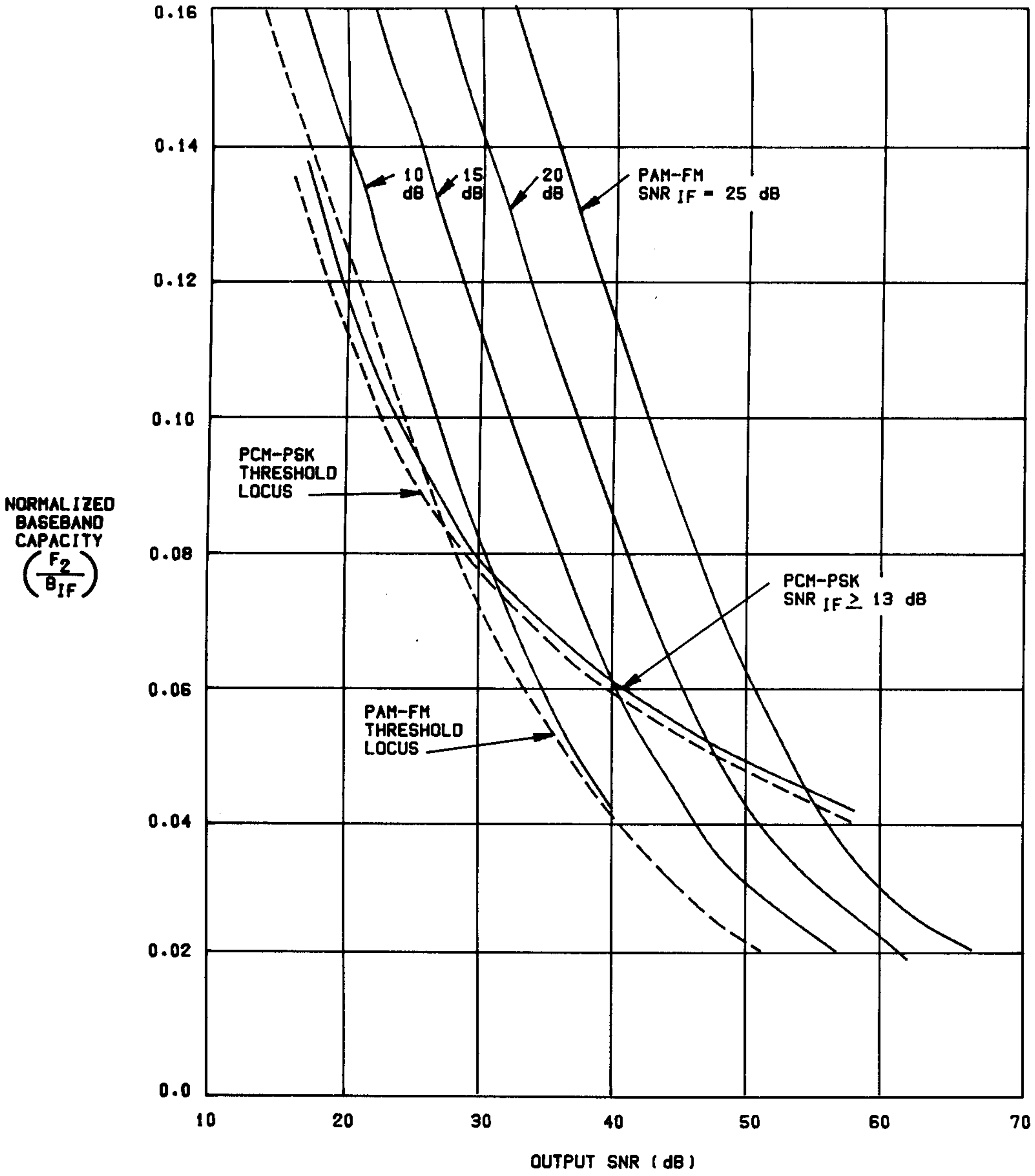


Figure 12 - Bandlimited Performance of PCM-PSK and PAM-FM Links

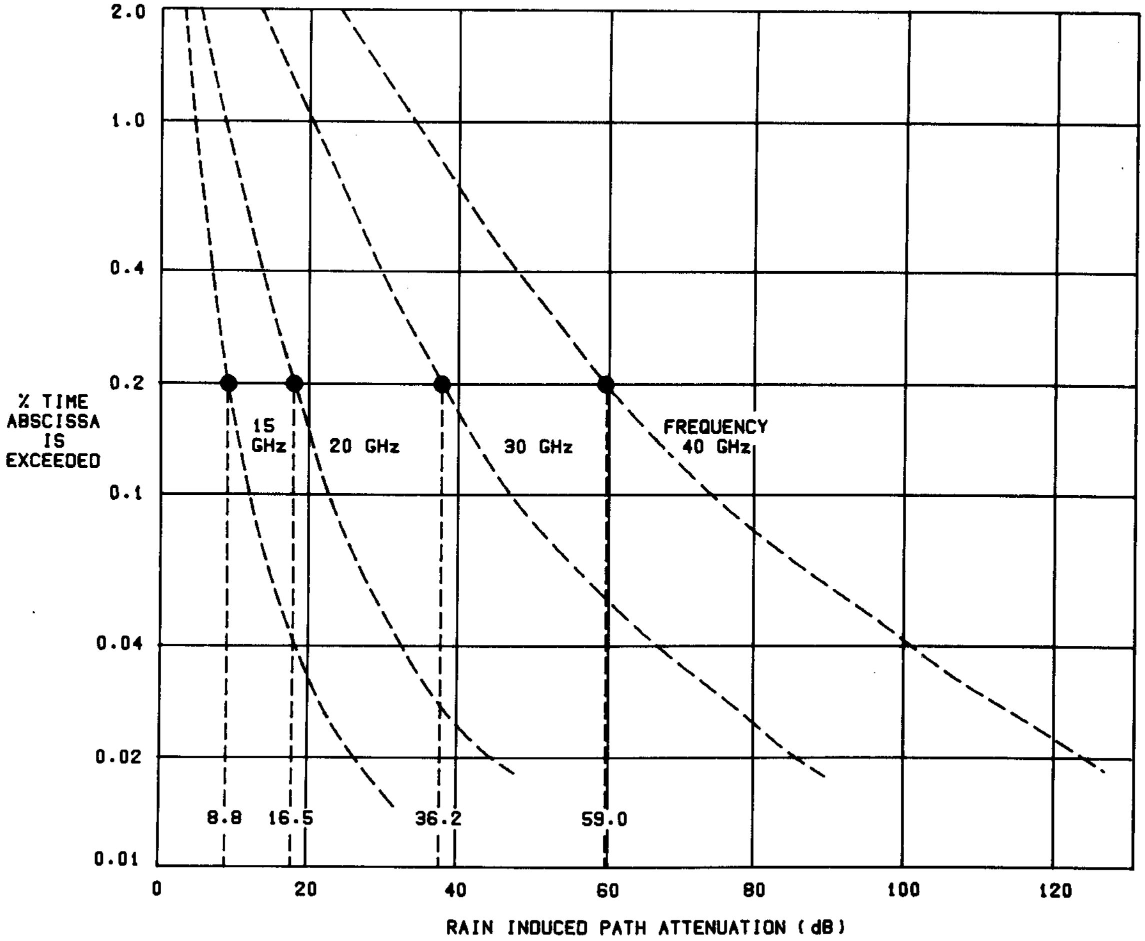


Figure 13 - Path Attenuation at 5° Elevation Angle - Various Frequencies

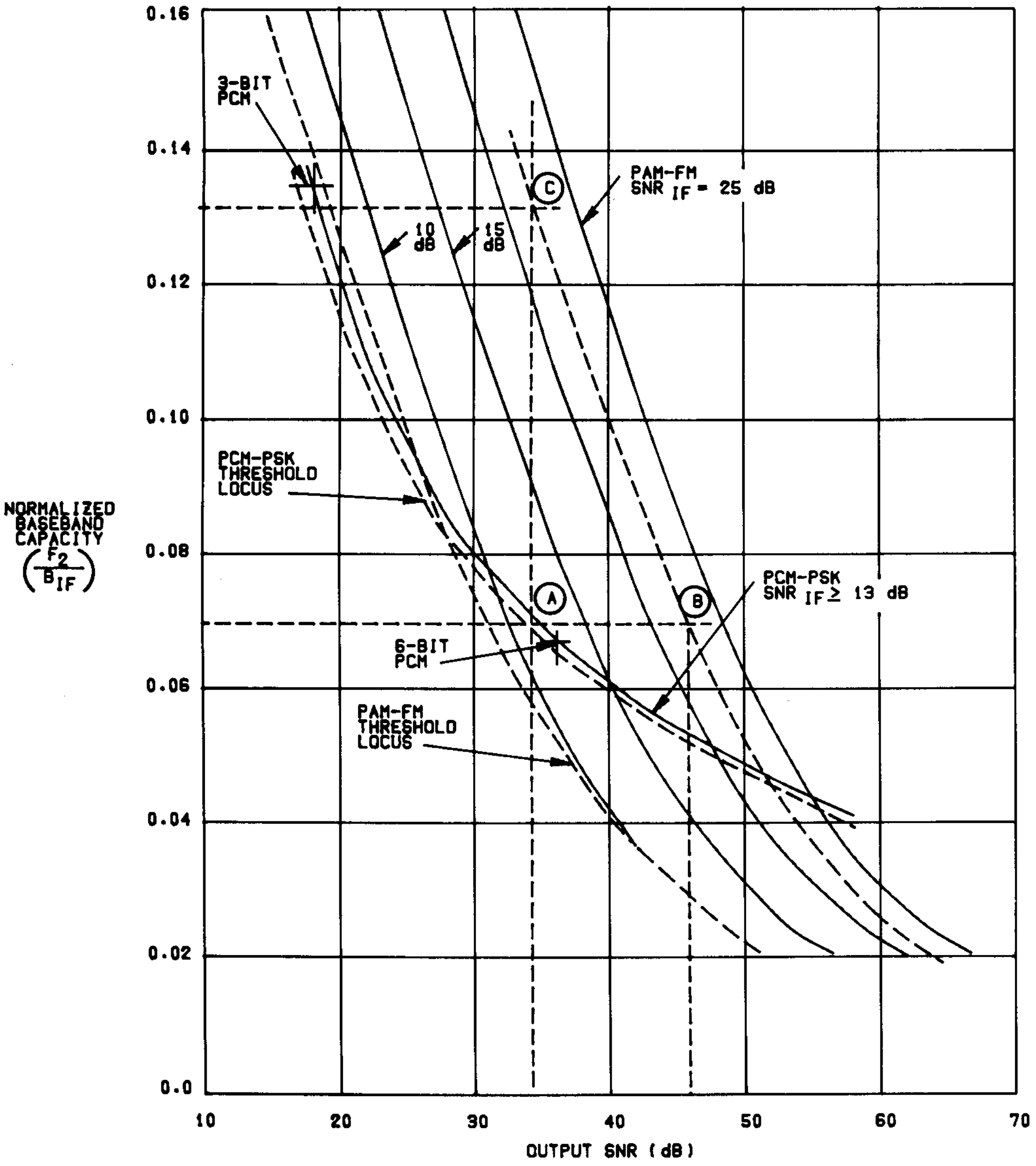


Figure 14 - System Design Example with Path Fading

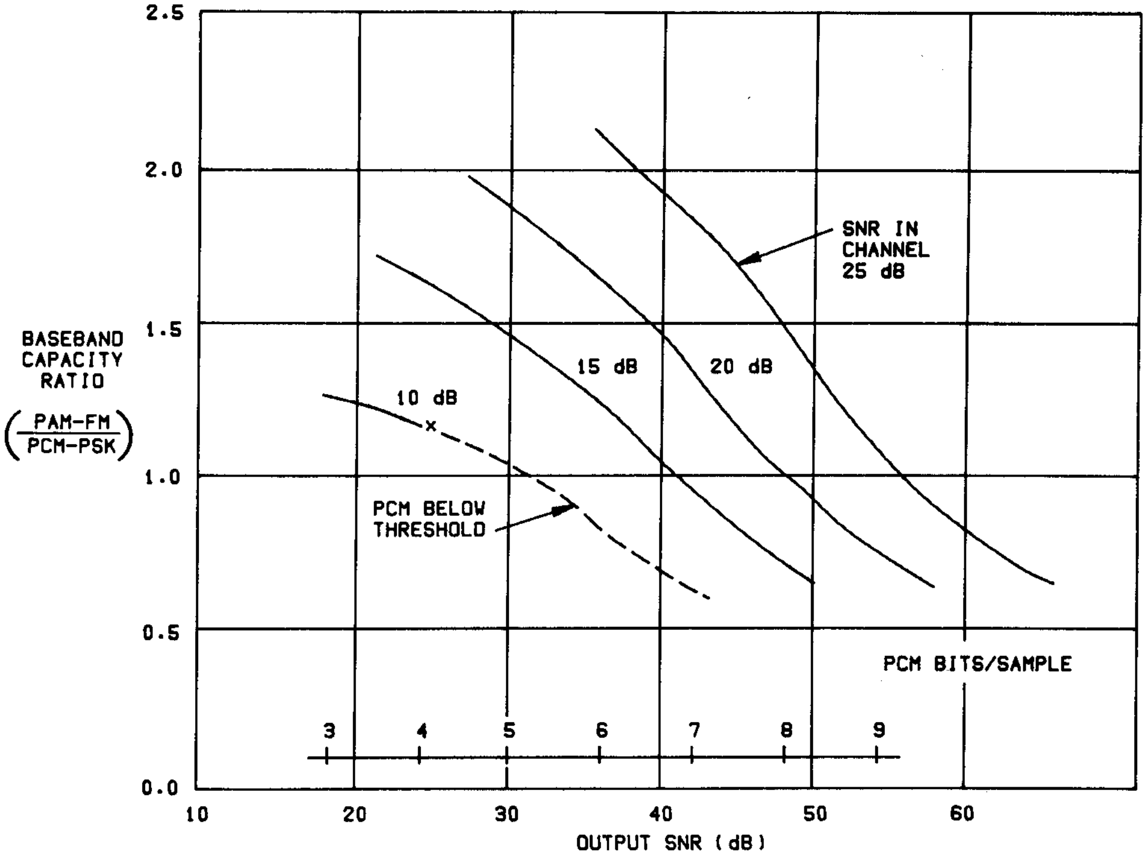


Figure 15 - Capacity Comparison in Bandwidth Limited Channel