When $P_b < 10^{-3}$, we may use the asymptotic approximation

$$\operatorname{erfc}(x) \cong [1/(\sqrt{2\pi}\ x)] \exp(-x^2/2). \tag{27}$$

Using (27) in both sides of (26) and taking the natural logarithm of both sides, we obtain

$$\ln a - [(E_b' - E_b)/N_0] = (1/2) \ln(E_b'/E_b). \tag{28}$$

We now approximate the right-hand side of (28) by the first term in a Taylor series expansion, that is, we use

$$\ln(E_b'/E_b) = \ln[1 + [(E_b'/E_b) - 1)]$$
$$\cong (E_b'/E_b) - 1, \tag{29}$$

which is reasonably accurate if

$$(E_b'/E_b) - 1 \ll 1. \tag{30}$$

Substituting (29) into (28) and employing the result in (24), we obtain the final expression,

$$D = 10 \log_{10} (1 + (\ln a)/(E_b/N_0) + 1/2)]. \tag{31}$$

In Fig. 4 of the previous paper,[1] the degradation is plotted for $n = 60$. The values of D from (31) are found to agree quite well with the plot.

It is easy to verify that (31) may also be used to calculate the degradation in word error rate. In this case, we replace (23) by

$$a = \begin{cases} [n + k - 2 - 2^{-k}(n - k - 2)]/k, & n \geqslant k \\ [n + k - 2 + 2^{-(n-1)}]/k, & n < k. \end{cases} \tag{32}$$

A comparison between (17) and (10) indicates that no member of the cryptographic ensemble suffers significantly more word error rate degradation than the ensemble average when $n = 60$ and $k = 10$. This statement is true for most practical values of n, k, and P_b. However, a comparison of (19) and (11) reveals the possibility that one or more members of the cryptographic ensemble may endure considerably greater bit error rate degradation than the ensemble average when $n = 60$. Substituting $a = n = 60$ into (22), it is seen that a member of the ensemble may have an extra degradation ranging from approximately 0.3 dB to 0.2 dB as P_b varies from 10^{-3} to 10^{-6}.

Section III

The statements following (28) of the previous paper must be modified. For a cryptographic system with a differential detector, the expressions for $P(w/tb = i)$ and $P(w/tb = k)$ are unchanged asymptotically, except when $tb = n = 1$. In this case, $P(w/tb = n = l) = 1$ because of the initial assumption.

Using the same methods previously employed, it follows that the asymptotic formulas for word and bit error rates of the differential cryptographic system are

$$P_{cb} = \begin{cases} [n + k - 1 - 2^{-k}(n - k - 1)]P_b, & n > k \\ (n + k - 1 + 2^{-n})P_b, & 1 < n \leqq k \\ (k + 1)P_b, & n = 1 \end{cases} \tag{33}$$

$$P_{cb} = \begin{cases} [(n + 2)/2)]P_b, & n > 1 \\ 2P_b, & n = 1. \end{cases} \tag{34}$$

A sufficient condition for the validity of these equations is given by (8) of the previous paper.

DON J. TORRIERI
Naval Research Laboratory
Washington, D.C. 20375

Discussion of "A Note on CEP's"[1]

The above recent correspondence[1] noted two approximations for CEP calculations; the first was concerned with an off-set (biased) circular Gaussian distribution and the second with a nonbiased elliptical Gaussian distribution. The purpose of this correspondence is to present an analytic approximation, which appears to be not well known, that handles both of these cases, along with a biased noncircular Gaussian distribution. The approximation may be utilized to handle a biased three-dimensional noncircular Gaussian case. The proof, given in a paper by Grubbs,[2] is based on a moment-matching technique of the probability density function for $R^2 = X_1^2 + X_2^2$ to an approximation chi-squared variate, followed by a Wilson-Hilferty transformation to a normal variate.

For X_1 and X_2 Gaussian distributed with means b_1, b_2 and variances σ_1^2, σ_2^2, the distribution function for $R = \sqrt{X_1^2 + X_2^2}$ is given by determining

$$F_R(r) = \text{Prob}\ [X_1^2 + X_2^2 \leqslant r^2].$$

The analytic approximation to this distribution function is given by

$$F_R(r) \cong (1/\sqrt{2\pi}) \int_{-\infty}^{f(r)} e^{-x^2/2}/2dx \tag{1}$$

where

$$f(r) = \left\{(r^2/m)^{1/3} - [1 - V/(9m^2)]\right\}\ [V/(9m^2)]^{1/2} \tag{2}$$

with

$$m = \sigma_1^2 + \sigma_2^2 + b_1^2 + b_2^2$$
$$V = 2(\sigma_1^4 + \sigma_2^4) + 4(\sigma_1^2 b_1^2 + \sigma_2^2 b_2^2).$$

[1] J. Bell, *IEEE Trans. Aerospace and Electronic System*, vol. AES-9, pp. 111-112, January 1973.

[2] F.E. Grubbs, "Approximate Circular and noncircular offset probabilities of hilting," *Operations Research*, vol. 12, pp. 51-61, January-February 1964.

Manuscript received January 23, 1974.

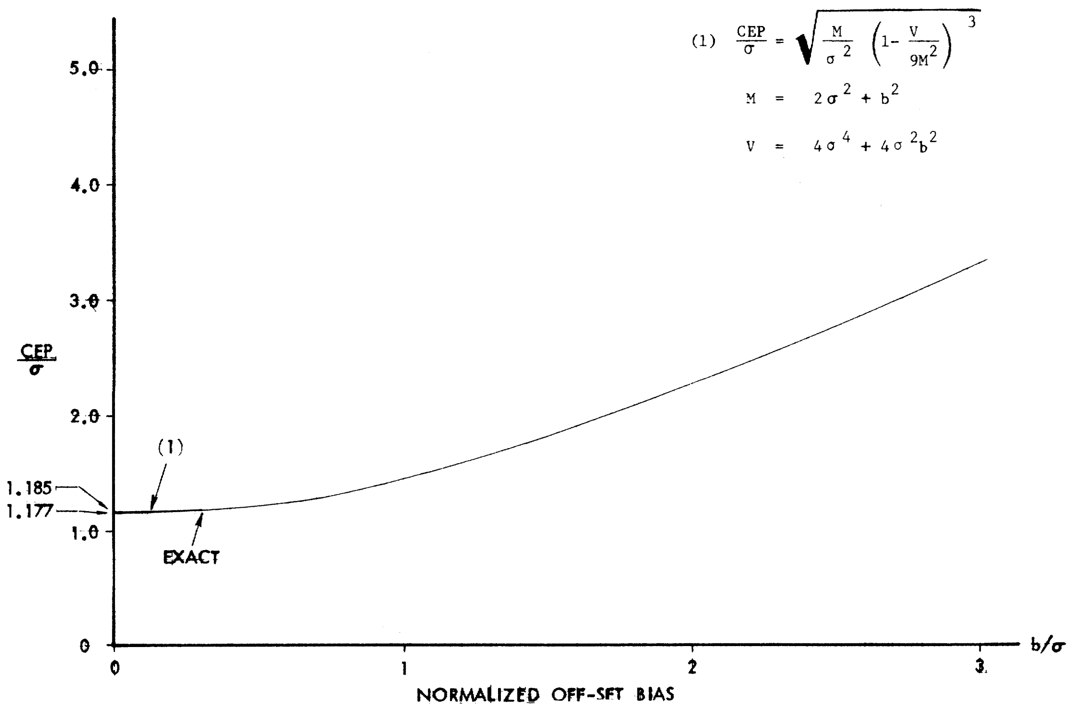

Fig. 1.

To obtain the desired CEP implies that $f(\mathrm{CEP}) = 0$. Solving (2) yields

$$\mathrm{CEP} = \sqrt{m[1 - V/(9m2)]^3}. \tag{3}$$

Fig. 1 illustrates the approximation given by (3) for the circular case; i.e., $\sigma_1^2 = \sigma_2^2 = \sigma^2$ with $b_1 =$ and $b_2/\sigma = 0, 1, 2, 3, \cdots$.

The extension to the three-dimensional case for SEP calculation is clear. It should be noted that (1) allows for the computation of any r at any desired probability level, and may be easily programmed utilizing one of the several numerical approximations for the integral of the normal density function. There are no constraints on the off-set values and, as such, (1) is extremely general. The one limitation found in practice is that the relative accuracy for probabilities less than about 0.10 may be low, and so the usefulness of (1) for this range of probability calculations is dubious.

R.C. TERZIAN
TRW Systems Group
Redando Beach, Calif. 90278

The Moon as Source For G/T Measurements

Abstract

For large-aperture antennas, it is customary to utilize radio stars in order to determine the receiving gain to temperature ratio. In the case of small-aperture antennas, which not only have reduced gain but usually higher system noise temperature as well, the *y* factors obtained from the radio star measurements are so small that the measurement error is intolerable. The moon, on the other hand, provides a power flux density higher by at least one order of magnitude compared to the strongest radio star, and the resulting *y* factors are usable. *G/T* ratios determined from moon measurements agree well with expected values.

Manuscript received February 28, 1974.

Introduction

The need for calibrated RF sources for the gain to temperature ratio measurement of the medium size antennas operating in the common carrier band calls for an investigation regarding the usefulness of the moon for such a purpose. It may appear on first glance, that the moon is a very undesirable source because of extended source size, the lunar phases, and finite time-varying distance. Yet, if proper account has been taken for the time-dependent variables, and if correction factors have been applied to compensate for extended source size, then the resulting G/T ratio is reasonably accurate. The degree of accuracy depends on how precisely the true distance from the station location to the moon at the time of test has been calculated and/or how well the gain pattern of the antenna under test is known. It is estimated and shown by comparison with independent gain and temperature measurements that the maximum relative error is within ± 0.25 dB.

Moon's Surface Temperature

The moon's radiation is indirect. The moon reradiates solar energy. Its temperature changes with lunar phases according to