SECRET

Copy No. 12

C E S G

COMMUNICATIONS-ELECTRONICS SECURITY GROUP

Research Report No. 3007

THE POSSIBILITY OF SECURE NON-SECRET ANALOGUE ENCRYPTION

SECRET

CESG REPORT NO. 3007

THE POSSIBILITY OF SECURE NON-SECRET ANALOGUE ENCRYPTION

J. H. ELLIS

Summary

This Report considers how secure non-secret encryption can be achieved by analogue means over direct metallic connexions of high quality. It describes a very cheap simple system, which suffers from a serious security defect but which might be of value in special circumstances. High-grade security is shown to be obtainable but no practical solution is offered.

Case No. 305 refers

Date of approval for issue:

May, 1970

Contents:

	Page
INTRODUCTION	3
POSSIBILITY OF NON-SECRET ENCRYPTION	4
THE ADDITIVE NOISE SYSTEM	4
CASE OF COMPLETE ACCESS BY INTERCEPTOR	6
THE "ACES" PARADOX	8
POSSIBILITY OF APPLICATION TO A REAL COMMUNICATION SYSTEM	10
CONCLUSIONS	13
REFERENCES	14
APPENDIX I	15
APPENDIX II	20

Enclosures:

Drawing Nos. Z32490, Sheets 1–8

INTRODUCTION

1. It is generally regarded as self-evident that, in order to prevent an interceptor from understanding a message which is intelligible to the authorised recipient, it is necessary to have some additional information initially known both to the sender and the recipient but kept secret from the interceptor. This information can take one or more of many forms, such as the encipherment itself, the construction of a cipher machine, a key setting or a one time tape. All these methods require a separate route by which such secret information can be sent without fear of interception, for only then can the cipher text be sent safely in a non-secret manner. Large quantities of cipher text of high security thus tend to need the parallel transmission of smaller, but still substantial, quantities of secret information. It was demonstrated in a previous report (Reference 1) that such secret information is not theoretically necessary and that, in principle, secure messages can be sent even though the method of encipherment and all transmissions of cipher text between the authorised communicators are fully known to the interceptor. This is what is meant in the title by "Non-secret Encryption".

2. Reference 1 dealt with digital transmission; the present paper considers how these results may be obtained by analogue means. The terms "analogue" and "digital" are not precisely defined, but the methods described in this paper are essentially different from those described in Reference 1 and thus are best considered separately; broadly, they are concerned with the physical characteristics of the link. For the sake of completeness the arguments of Reference 1 will be repeated here where necessary.

3. The arrangement of this Report is as follows. The next section discusses general principles and the following section ("The Additive Noise System") describes a specific method of achieving some of the aims using a simple technique. This method has a severe security weakness, however, when the interceptor really has complete access to the communications. The problem of providing high-grade security under these conditions is then discussed in the section "Case of Complete Access by Interceptor" and this leads to the apparent impossibility of so doing, for all definite information about the state of the sender's equipment known to the recipient must also be known to the interceptor. The section "The Aces Paradox" describes principles by means of which this apparent impossibility can be circumvented and illustrates these by the well-known probability paradox referred to in the title. "Possibility of Application to a Real Communication System" deals with methods of applying these principles in a practical case and the conclusions are summarized in the last section. Mathematical analyses and experimental results are contained in the two appendices.

POSSIBILITY OF NON-SECRET ENCRYPTION

4. In all that follows the originator of the message will be referred to as the "sender", the authorised recipient as the "recipient" and the clandestine interceptor as the "interceptor".

5. Clearly if the recipient is to read the message he must be in some special position with respect to the interceptor. As they are both presumed to know the cipher text equally, this would seem to imply that the recipient has some knowledge denied to the interceptor and also that this knowledge must be shared by the sender (otherwise how could it be put to use?). The idea that the recipient might be in this special position purely because he is the authorised recipient does not seem possible; but consider the following case.

6. An ingenious scheme intended for the encipherment of speech over short metallic connexions was proposed by the Bell Telephone Laboratories, (Reference 3), in which the recipient adds noise to the line over which he receives the signal. This is illustrated in Figure 1a. If this noise is sufficiently large compared with the message it can effectively disguise it. The recipient however can subtract the noise from the signal he receives and so obtain the original message. This method has an important property. If the interceptor were provided with a receiver identical with that of the recipient and connected to the same point on the line, then the two terminals would be identical for all practical purposes and could be interchanged without altering the situation. However, the interceptor would not be able to read the message, as he would not know the noise which had to be subtracted from the line signal. Thus this system fulfils the condition which was discussed above that the recipient is able to decipher the message because he is the authorised recipient and not because of any special physical position or prior secret knowledge. Clearly if the interceptor tries to obtain the message by pretending to be the recipient and also adding noise to the line, all that he will do will be to prevent the genuine recipient from getting the message, and he will reveal his presence without obtaining any information.

7. In Reference 1 the essential ideas of the above discussion were applied to messages transmitted by normal digital means. The present report is restricted to direct developments of the additive noise system and in all that follows direct metallic connexions of high quality will be assumed.

THE ADDITIVE NOISE SYSTEM

8. We shall now consider the properties of the additive noise system. A simple practical method of implementation is shown diagrammatically in Figure 1b. In this a noise generator N feeds its signal both into the line and into a second terminal of a differential amplifier. It is easily seen

that the output from the differential amplifier will consist of the original signal inverted, provided that the two potentiometers formed by R and Z are correctly balanced. Z is the impedance of the lines as seen from the receiving end and will closely approximate the impedance of the transmitter since a short metallic connexion is assumed. It will be seen that it is essential for the receiver to know this impedance Z in order to compensate for the added noise. However as this is essentially the output impedance of the transmitter it can be standardised.

9. The obvious disadvantage of this system is that the noise necessary adequately to disguise the message is very large and it may therefore be necessary to reduce the normal working level of the transmission substantially to avoid overloading the line. In conditions of good signal-to-noise ratio which we are considering this should be possible, but it is still undesirable as very high noise-signal ratios would be required to be seen by the interceptor before good security could be assumed, and the higher is the amount of added noise then the more precise is the compensation required to remove it. This difficulty can be avoided by a simple modification to the scheme. It will be observed that, providing the compensation is correctly adjusted, the output from the amplifier is unaffected by the noise generated by N. Anything we wish can therefore be added to N. If then we add the message itself to N in such a phase as to cancel the message in the line signal the line signal will have no message component and will consist only of noise. Theoretically, of course, the noise is no longer necessary as there is no line signal to disguise but this would require perfect cancellation and thus it is best to use cancellation plus noise. In this way the level of noise and the precision of noise cancellation needed can be kept low.

10. It is shown in Figure 2, parts a – c that the process of feeding the output of the amplifier back in such a way as to cancel the line signal and compensating for this by feeding the output also into another input is equivalent to using a high gain feed-back amplifier. An arrangement of this form is shown in Figure 2d, and it will be observed that no precise adjustment is necessary in order to cancel the line signal, although for cancellation of noise in the receiver output Z_1 must be equal to Z_2.

11. A peculiarity of the signal cancellation process is that the line signal seems to have disappeared and then reappeared out of nowhere. It is indeed true that the amplified input is effectively short-circuiting the line and that an interceptor could obtain no information from the voltage at this point. However this short-circuiting effect is obtained by matching exactly the signal current with its complement and thus the current is available to reproduce the recipient's signal. Viewed from the line the receiving apparatus appears to be a low impedance noise source.

12. Considered in this way the security weakness of this system is apparent; the original message is contained in the line current although it has been effectively cancelled from the voltage. If an interceptor measures both the voltage and the current and combines them in the appropriate ratio he will be able to cancel out the noise and obtain the original signal.

13. A practical model of this system was constructed and the circuit is shown in Figure 3. An analysis and experimental results are given in Appendix I and it will be seen that apart from the major disadvantage of the possibility of current cancellation this system has some remarkable advantages. It is small, convenient, needs no key setting or synchronisation and is so cheap (it would only cost a few pounds per terminal) that its expense would be negligible. Moreover, if it were used in the situation where the link consisted of a good metallic connexion of only a few hundred yards, and an interceptor were prevented by some means from gaining access to the current, then the security is demonstrably high-grade.

CASE OF COMPLETE ACCESS BY INTERCEPTOR

14. We see from the above section that devising a system where the interceptor and recipient can occupy identical positions with identical prior knowledge is not sufficient. In the added noise method the recipient is able to obtain the sender's message without using all the information on the line, but this does not mean that the interceptor is necessarily restricted in the same way, and in this case we have seen that if he does obtain all the information, i.e. the voltage and the current, he can also readily obtain the original message. The next question to consider therefore is whether we can devise a system in which the interceptor is unable to read the message, even though he has access to all the information flowing between the two authorised communicators. If not one might regard the above system simply as a trick in which the information is transmitted by current instead of voltage, and thus the unwary interceptor would be outwitted, but only so long as he did not realise what was happening. In this view the method is of no more value than that of sending a message on one route while pretending to send it on another. (It is clear, of course, that the plain added noise system without signal cancellation can also be broken by this technique). We shall now therefore examine the problem of providing genuine security.

15. We shall avoid considerations of a complex cipher-type dialogue between the two communicators, as this would, in effect, reduce to the digital case considered in Reference 1. We shall confine ourselves to examining the question of whether the recipient can read the signal sent by the sender, or at least a vital part of it, without the interceptor being able to do so.

16. First let us establish the essential nature of our communications system. By Thévenin's theorum, either communicator can be represented by a voltage in series with an impedance. For

simplicity let us first regard these as simple instantaneous voltages and resistances. This gives us the arrangement shown in Figure 4, in which the send and receive voltages are called e_1 and e_2 respectively, the send and receive resistances r_1 and r_2 respectively and the line current and voltage i and e. The essential relationships between these components are given by the equations

$$e = e_1 - ir_1 = e_2 + ir_2$$

17. If r_2 is zero, then we have the case of additive noise with signal cancellation, in which all the message signal e_1 is contained in i. If r_2 is large we have the simple noise additive system of Figure 1 in which the message information is mainly contained in e; if r_2 is made infinitely large, then all the information is contained in e.

18. It is thus clearly possible to vary the proportions of signal information carried in i and by varying r_2, and at first sight it might seem that doing this rapidly in a random manner would hide the intelligence. However solving for e_1 gives us

$$e_1 = e + ir_1$$

This does not contain r_2 and therefore this added complication is of no security value, as noise cancellation depends only on knowledge of r_1 and can be carried out as before.

19. If then e and i are both known, a linear relationship is established between e_1 and r_1 so that if one is known the other can readily be deduced. Therefore it will be necessary for the sender to vary both e_1 and r_1 if he wishes to disguise his message, and this message will have to be deduced by the recipient from knowledge of the values of e and i. However the knowledge of e and i specifies that the pair of values e_1 and r_1 lie on the straight line $e = e + ir_1$ as shown in Figure 5a. This information is supposed to be known equally to the interceptor, and thus we have the condition that, although the recipient has some control over e and i by varying e_2 and r_2, the actual information available to him is only that the position of the e_1, r_1 pair lies on the specified straight line and this information is also known to the interceptor. Complicating the position by using complex forms of e and r, leads to similar results, and thus at first sight it would seem that the objective of secure non-secret communication was unobtainable by these means.

20. This conclusion rests on the 'obvious' hypothesis that if two people have the same information they can obtain the same conclusions from it. For this purpose we do not regard the knowledge of values of e_2 and r_2 as information, since the knowledge which can be obtained from e and i is that the values of e_1 and r_1 lie on a specific line and this is true whether or not e_2 and r_2 are known. Put in another way, both the interceptor and recipient have the same definite

information about the message, although the recipient has some additional information about the way in which the information was obtained, namely about the values of e_2 and r_2.

THE "ACES" PARADOX

21. To attempt to exploit this unpromising situation we shall investigate the paradox that the value of information may be dependent upon the way in which this information was obtained, even though the truth of the information is not in doubt.

22. To illustrate the principle involved we shall consider the well-known paradox of the second ace. In this two cards are dealt from a normal pack of 52 and the problem is to determine the probability that they are both aces, given that one of them is the ace of spades. First consider the case where the information has been obtained by asking the question "Have you the ace of spades?" to which the answer was "Yes". There are 51 ways of holding two cards of which one is the ace of spades and three ways of holding two aces including the ace of spades; therefore the probability of holding two aces in these circumstances is 3 divided by 51 or one-seventeenth. If however the information had been obtained by asking the questions "Have you an ace? If so, what is it?" to which the answer was "The ace of spades" we obtain a different probability. Clearly the fact that the ace which is held is the ace of spades is of no importance; therefore we know merely that one ace is held and our problem becomes that of calculating the probability of holding two aces given that at least one is held. The number of ways of having two cards is 26×51. The number of ways of having no aces is 24×47. Therefore the number of ways of having at least one ace is the difference between these two numbers, which is 198. The number of ways of holding two aces is six and therefore the probability of having two aces, given that one is held, is 6/198 or 1/33. These two probabilities are substantially different and are obtained from the same information, the only difference between the two cases being the way in which the information was obtained, i.e. in the kind of questions asked.

23. This demonstration is quite genuine but may seem unconvincing at first. We shall avoid trying to give fundamental explanations but try to make the mechanism more obvious by using a simplified example. Consider the case in which a pack of three cards only is used. Let these cards be the ace of spades, the ace of hearts and the two of clubs. Clearly, the probability of two aces being dealt in a random selection of two cards is one-third, and the probability of there being two aces, if the ace of spades is known to be dealt, is one-half because there are only two possibilities. If then the question "Have you the ace of spades?" receives an affirmative answer there is a probability of one half that two aces are held. On the other hand, the question "Have

you an ace?'' is of no value, since at least one ace must always be held, and the further information that this ace is the ace of spades, if in reply to the question, ''What is your ace?'' is likewise of no value; therefore in this case the probability of two aces being held is one-third.

24. The probability of a second ace being held thus depends on the questions which were used to elicit information about the one ace held, and it is quite simple to devise a secure means of transmitting information based on this fact if the questions are unknown to an interceptor.

25. We can do this as follows. Firstly the presence or absence of the second ace can be controlled by a single bit of information which the sender wishes to convey to the recipient. The recipient has a pack of three cards, the aces of spades, hearts and clubs. Depending on the value of the current bit of information he deals himself either one or two of these aces. The recipient has now to find out whether one or two aces has been dealt by asking questions which are supposed not to be available to the interceptor, although the choice of question is known. The questions available are:-

a. Have you the ace of spades?
b. Have you the ace of hearts?
c. Have you the ace of clubs?
d. Name an ace which you have.
e. Name an ace which you have not.

The sender's reply to these questions is always of the form, ''I have the ace of'', or ''I have not the ace of''. In this way the only definite information transmitted is available to the interceptor.

26. It is easily seen that the answer, ''I have the ace of'', to questions a, b, or c, gives a probability of two-thirds of there being two aces, while the answer ''I have not the ace of'', gives a probability of one-third. Answers to the other two questions give no useful information.

27. By proceeding in this manner a number of times for each bit of information to be transmitted the recipient can establish its value with a high degree of probability. The questions d and e are included so that the distribution of the two kinds of answers can be balanced at will by the recipient, as the kinds of answer to these two questions are clearly known in advance. Without this provision the distribution of affirmative and negative answers would convey as much information to the interceptor as to the recipient.

28. The essential features of this system are that the recipient asks unknown questions of a definite form and the sender replies with answers giving simple truthful information required by the question. There is no question of coding, or answers of a "yes" or "no" form, which depend for interpretation on the question. The point is that at no stage is any definite information given to the recipient, but he is able to make a better assessment of the probabilities of the sender's situation than the interceptor because he knows the question and the question limits the kind of answer possible.

POSSIBILITY OF APPLICATION TO A REAL COMMUNICATION SYSTEM

29. The system of Figure 4 is analogous to the above situation in that the values of e_1 and r_1 correspond to the cards which have been dealt, the values of e_2 and r_2 to the questions and the values of i and e to the answers. The above considerations imply that a secure transmission of information should be obtained by varying e_1 and r_1 according to the information which is to be transmitted, and varying e_2 and r_2 so that the probabilities of the original information can only be deduced from i and e by knowing e_2 and r_2.

30. To try to formulate a practical system from these rather vague ideas let us examine Figure 5. Figure 5a shows the locus of possible positions of e_1 and r_1 for a given e and i; Figure 5b shows the corresponding locus for e_2 and r_2 but the value of r_2 has been shown negative in order that the two loci may be identical. Combining Figures 5a and 5b gives 5c, in which the vertical axis represents values of e_1 and e_2, and the horizontal axis values of r_1 and $-r_2$. If r_1 and r_2 have only positive values then the e_1, r_1 pair will always lie on the right hand side of the diagram and e_2, r_2 on the left. In practice therefore both the interceptor and the recipient know the position of the locus which defines the possible positions of e_1, r_1 and e_2, r_2. In addition they would both be assumed to know any conventions or *a priori* probabilities of the positions of e_1, r_1, and the recipient would know the position of e_2, r_2.

31. It may be possible to devise a satisfactory scheme while limiting the resistances to positive values but it is very restrictive, and as it is clearly possible by the use of reactances or other means to obtain negative impedance which can be used in the same way as the resistances this restriction will be assumed to be removed in the following discussion. Therefore we can describe the situation geometrically as one in which both the sender and recipient specify a point in the plane, and the resulting line joining these two points is known both to the interceptor and recipient. The problem is then one of determining how to manoeuvre these points so that information can be conveyed without being given away to the interceptor by the positions of the lines.

32. There are a number of ways in which this could be done in principle. Consider for example the case in which both points were restricted to lie on a given circle. The resulting locus would therefore be a chord of this circle and the intersections with the circle therefore determine the two points, but the recipient would know which end was his point and therefore the exact location of e_1, r_1. The interceptor, however, would only know that e_1, r_1 was one of a pair of points and it would be possible to devise a scheme to make use of this difference of knowledge. This differs somewhat from the card-guessing analogy in that a definite answer is in fact obtained by the recipient; however this is merely a limiting case which could in fact be parallelled by taking an infinite number of cards. As this particular method does not seem to have any practical merit it would not be considered further, but we will proceed to the general case.

33. For brevity we shall hereinafter refer to the point e_1, r_1 as s_1 and the point e_2, r_2 as s_2. In order to convey information it is necessary that the probability distribution of s_1 vary according to the message to be transmitted.

34. Consider for simplicity the case of two alternative distributions corresponding to one bit of information. Let these distributions be A and B, then for either case and for a particular s_2 the probability of the locus being in a particular direction is proportional to the integral of the probability density per unit angle as measured from s_2 in that direction. The probabilities for directions differing by π are of course added as there is no means of telling on which side of s_2, s_1 lies.

35. Turin's theorem Reference 2 states that the posterior odds of a hypothesis being true are given by the prior odds of it being true multiplied by the ratio of the probabilities of an observed result happening in the cases where the hypothesis is true and where it is false. In other words:-

$$\text{Posterior odds} = \frac{\text{Probability of result if hypothesis is true}}{\text{" " " " " " false}} \times \text{prior odds}$$

36. In the present case we may take the hypothesis as being that the probability distribution s_1 corresponds to A. Initially the prior odds may be taken as one, so that the odds in favour of Case A being true (i.e. that s_1 is determined by distribution A), after the first trial, are given by the probability of the locus resulting from Case A divided by the probability of it resulting from Case B. These odds of course become prior odds for a second try and we see that the ultimate odds can be computed as the product of the factors resulting from a series of tries. In the manner usual with the factor method. Thus the decision as to whether the sender is using distribution A or B can be made with a certainty dependent on the number of trials and the size of the factors obtained from them.

37. For this method to be effective it is obviously necessary that the probabilities should be substantially different in the two cases and that they should be heavily dependent on the position of s_2. If this latter condition is not fulfilled then clearly the interceptor will be able to obtain enough information to read the message.

38. It might appear that there can be no dependence of the probability on the position of s_2, on the grounds that the integral of the probability density along the length of the locus does not involve this point. But from the point of view of the recipient the probabilities are those of a vector passing through a fixed point being in a certain direction. Thus the probability of a locus occupying a certain position is proportional to the probability density per unit angle of this locus in that position, and this is clearly equal to the integral of the product of the probability density along the locus multiplied by its distance from s_2 (the distance always being taken as positive). Thus the further s_2 is from regions of high probability density along the locus in a particular case, the higher is the probability of that case. To get a physical picture of this, consider the case where the locus passes through two small regions of high probability density, one in Case A and the other in Case B. If s_2 is located very close to the high region of Case A, then the most likely hypothesis is that Case B is being employed. For if it were Case A, a small variation of position within the region would change the position of the locus greatly, but if it were Case B, any position within the high density region would produce approximately the same result.

39. A possible implementation of this is illustrated in Figure 6. Here the probability distributions for s_1 in the Cases A and B correspond to the lines

$$e_1 + Ir_1 = k$$

$$e_1 + Ir_1 = -k \text{ respectively}$$

where I is a constant.

40. s_1 is moved about the plane in a random manner and the probabilities calculated as shown in Appendix II. It would be necessary to bias the positions of s_2 as the probabilities became more apparent in order to conceal the answer. This would be done by tending to put s_2 further from the line of higher probability and would correspond to the use of questions d and e in the aces example.

41. It will be seen from Appendix II that the solution of the probability problem given in this case is complex and although feasible it is by no means attractive. This example was of course chosen for its geometrical simplicity and it is to be hoped that a very much simpler solution in statistical terms can be found; but no attempt has been made to investigate this possibility.

42. Let us now consider some of the practical aspects of the process. The first of these is the problem of generating negative values of r_1 and r_2. Negative resistances are of course quite common, but the employment of two such, with random values, in series, would create great problems of stability and seems impracticable. Alternatively we may use alternating potentials and replace the resistances by reactances which can therefore have both signs. This would probably tend to cause slow transmission, as it would be necessary for some sort of equilibrium condition to be established at each trial. However this could be overcome by using a complex form of both e and r. e_1 and e_2 could be complex waveforms occupying a finite period and consisting of a large number of harmonics of the fundamental of this period; r_1 and r_2 could be complex impedances expressed in similar terms and thus many trials could be made at the same time.

43. This latter method has the substantial advantage that it would be very difficult for an interceptor to obtain extra information by active participation. In the case of simple resistance a sharp pulse of current or voltage applied to the line could give an interceptor a direct measurement of the resistances on either side of him and thus short-circuit the information-retrieval process. With a complex Fourier pattern to deal with, it seems unlikely that such a technique would be possible without upsetting the authorised communicators.

CONCLUSIONS

44. This report gives us two distinct conclusions. First we have the extremely cheap, simple and, under some circumstances, effective method of signal cancellation with added noise, and secondly we see that it is very likely that a secure system on the lines of the probability method described above could be developed. However, both these systems depend as we have said on the existence of short high-quality metallic connexions and are thus amenable to encipherment by the cheapest of the traditional methods. There would be no transmission problems and little problem in communicating secure key settings. Thus the usefulness of these techniques depends on their being developed in a cheap simple form. The first, of course, meets this requirement ideally but there is no quarantee at the moment that the second form could be made cheaper than a traditional key generator. The usefulness of either system would therefore seem to need either further development or a special application.

45. A possible use of the first method would be in connexion with some form of non-cryptographic protection. So far no satisfactory form of NCP has been devised for cables outside protected areas, but these attempts have been concerned with preventing access to the line voltage In the signal-cancellation system it is necessary for the interceptor to monitor both current and

voltage and it may well be possible for it to be made very difficult for an interceptor to do this even though it were relatively simple for him to obtain the voltage only. For example, in a light guide it might be virtually impossible to measure light flux (as opposed to brightness), and in a coaxial cable formed by sputtering a thin film on to an enamelled wire the current could only be measured by completely breaking the outer conductor.

REFERENCES

1. J.H. Ellis
The Possibility of Secure Non-Secret Digital Encryption
CESG Research Report No. 3006, January 1970

2. I.J. Good
Probability and the Weighing of Evidence
Charles Griffin & Co. Ltd., 1950

3. Final Report on Project C43
Bell Telephone Laboratory, October 1944, p.23

APPENDIX I

Analysis and Experimental Results of the Signal-Cancellation System

Analysis

1. In Figure 2d, let the amplifier gain be A, the open-circuit line voltage (i.e. the voltage seen by the recipient when none of his apparatus is connected) V_1, the actual line voltage E and the receiver output V.

2. From the sum of the currents at E we have

$$\frac{V_1 - E}{Z_1} + \frac{V - E}{R_2} + \frac{N - E}{R_1} = 0$$

and from the fact that V is A times the sum of the amplifier inputs we have

$$\frac{V}{A} = \frac{NR_2Z_2}{R_1R_2 + R_1Z_1 + R_2Z_2} - E$$

These equations can be written, after simplification, as

$$\frac{VY_2}{A} = \frac{N}{R_1} - EY_2$$

and

$$EY_1 = \frac{V_1}{Z_1} + \frac{V}{R_2} + \frac{N}{R_1}$$

Where

$$Y_1 = \frac{1}{Z_1} + \frac{1}{R_1} + \frac{1}{R_2}$$

and

$$Y_2 = \frac{1}{Z_2} + \frac{1}{R_1} + \frac{1}{R_2}$$

Eliminating E gives

$$V\left(\frac{Y_1}{A} + \frac{1}{R_2}\right) = -\frac{V_1}{Z_1} + \frac{N}{R_1}\,\frac{Y_1 - Y_2}{Y_2} \qquad (1)$$

and eliminating V gives

$$EY_2\left(\frac{Y_1}{A} + \frac{1}{R_2}\right) = \frac{V_1Y_2}{Z_1A} + \frac{N}{R_1}\left(\frac{1}{R_2} + \frac{Y_2}{A}\right) \qquad (2)$$

3. If we denote the value of V when $Y_1 = Y_2$ by V_0 we get from *(1)*

$$V_0\left(\frac{Y_2}{A} + \frac{1}{R_2}\right) = -\frac{V_1}{Z_1} \quad \left(or\ -\frac{V_1}{Z_2}\right)$$

and if we call E_0 the value of E when A is infinite we get from *(2)*

$$E_0 = \frac{N}{R_1 Y_2}$$

4. The signal/noise voltage ratio of V is the ratio of the component due to V_1 and that due to N. From *(1)* this is

$$(S/N)_v = \frac{V_1}{Z_1} \times \frac{R_1}{N} \times \frac{Y_2}{Y_1 - Y_2}$$

$$= \frac{V_1}{Z_1} \times \frac{1}{E_0} \times \frac{1}{Y_1 - Y_2}$$

$$= \frac{V_1}{E_0} \frac{Z_2}{Z_2 - Z_1}$$

5. From *(2)* the signal/noise voltage ratio of E is

$$(S/N)_E = \frac{V_1}{Z_1\left(\frac{Y_2}{A} + \frac{1}{R_2}\right)} \times \frac{Y_2 R_1}{N} \times \frac{1}{A}$$

$$= \frac{V_0}{E_0 A}$$

6. From these results we see that the residual noise in the output is proportioned to the unbalance of Z_1 and Z_2 and is not affected by A; also the residual signal component on the line is inversely proportioned to A and is not affected by the Z balance. These results are exact; no approximation has been made nor any assumption about values. Also it may be noted that the expression for V_0 does not require infinite A, neither does that for E_0 require that $Y_1 = Y_2$.

7. In practice A was greater than 25,000 and the Z balance better than 40 dBs so we may write to a suitable approximation.

$$V = V_0 = -\frac{V_1 R_2}{Z_1}$$

and $$E = E_0 = \frac{N}{R_1 Y_2}$$

This makes $$(S/N)_v = \frac{V}{E} \frac{Z_2}{Z_2 - Z_1}$$

and $$(S/N)_E = \frac{V}{E} \times \frac{1}{A}$$

8. If R_1, R_2 and Z_1 are nominally equal we get

$$V = -V_1$$

and $$E = N/3$$

9. The approximate results are, of course, obvious by inspection but the somewhat cumbrous derivation clarifies the exact nature of the approximation. These show that, in the practical case where $A > 25{,}000$, the signal voltage at the input to the receiver is attenuated by an amount of the order of 90 dBs; and so, for all practical purposes, the receiver can be regarded as a zero-impedance source of voltage E. Thus no information will be available to an interceptor from the voltage at this point. Now let us consider the condition on the line nearer to the transmitter.

10. Clearly the further the point of measurement is from the receiver the greater will be the signal component and the less the noise. As the attenuation must be small we can neglect the variation of noise along the line. To a very close approximation the signal component will be $\frac{V_1 Z_S}{Z_1}$; where Z_S is the impedance of the portion of the line between the point of measurement and the receiver, with a short-circuit at the receiver. As Z_S will be greatest at the transmitter this place will give the worst-case condition and will be the assumed point of measurement in what follows.

11. As the noise will be substantially the same as at the receiver we can take it as being E_0 with negligible error. If we call the signal/noise ratio at the transmitter $(S/N)_T$ we have

$$(S/N)_T = \frac{V_1 Z_S}{Z_1} \times \frac{1}{E_0}$$

and if we take $(S/N)_V$ in the form $\frac{V_1}{Z_1} \times \frac{1}{E_0} \times \frac{1}{Y_1 - Y_2}$ we see that

$$\frac{(S/N)_V}{(S/N)_T} = \frac{1}{Z_S(Y_1 - Y_2)}$$

12. This is the improvement in signal/noise ratio from the line signal at the transmitter to the final received signal. This a figure of merit of the system as the signal/noise ratio of either signal can be arbitrarily altered by changing the ratio V_1/E_0. Moreover, $Y_1 - Y_2 = 1/Z_1 - 1/Z_2$, and Z_1 essentially consists of the open-circuit impedance of the line (which we shall call Z_0) in parallel with the output impedance of the transmitter. Therefore, as the latter will be resistive and easily matched, we may take $1/(Y_1 - Y_2)$ as approximately Z_0/d where d is the proportional error in matching Z_0 in Z_2.

13. d will be a matter of care of adjustment, and will be little effected by the magnitude of Z_0, so that Z_0/Z_S is a figure of merit for the cable. In other words, the ratio of signal/noise ratio of the final signal to that of the line signal at the point most favourable to the interceptor is proportional to the ratio of the open-circuit to short-circuit impedances of the connecting cable for a given precision of balance between Z_1 and Z_2.

14. Since we are concerned only with lines which are short relative to the wave-lengths of the signal components we may neglect inductive effects, and, so long as Z_0/Z_S is large, we may consider a simple lumped-constant model. This means that Z_S becomes the series resistance of the cable and Z_0 becomes the impedance of the capacitance. In order to optimise the figure of merit for the cable we have, therefore, to make the product of the resistance and capacitance a minimum.

15. A coaxial cable has the advantage that the current cannot be measured without breaking the outer conductor. The capacitance per unit length of a cable of inner radius a, outer radius b and dialectric constant k is $\frac{k}{2 \log \frac{b}{a}}$. The resistance per unit length is $\frac{P}{\Pi a^2}$ where P is the resistivity. (The resistance of the outer conductor being neglected). The product is therefore a minimum when $a^2 \log \frac{b}{a}$ is a maximum. This is easily seen to be when $\frac{b}{a} = \sqrt{e}$ for a given b. Thus the best result is obtained from a cable of given outer dimension and materials when the radii of the outer and inner conductors have a ratio of about 1.5.

16. In the case of the optimum ratio $2 \log \frac{b}{a} = 1$ and so the capacity per unit length = k. For polethene this gives a capacity of 2.3 pF/cm or 21 nF per 100 yards. If the inner conductor is chosen to be 14 S.W.G. wire, which gives a very thin cable, then the resistance is half an ohm per hundred yards. Therefore we could take Z_0 to be a capacitance of 0.2 μF per thousand yards and Z_S to be a resistance of five ohms per thousand yards as the basis of our calculations. This gives a value of 50 for Z_0/Z_S at 3000 Hz, and proportionately better at lower frequencies. With a value of 1/20 for d this would give an improvement in signal/noise rate of 40 dB at 3 kHz, improving by 6 dB/octave below this.

Experimental Results

17. The arrangement of Figure 3 was set up, and both V_1 and E were set at about 1 volt p/p. Z_0 was taken as 0.2 pF and Z_S as 10 Ω. Thus a somewhat conservative choice was made for the simulation of a thousand yard line. The noise was balanced out by adjusting the single potentiometer in the network feeding Z_2 and a precise null was found to be readily obtainable; the residual noise could be made scarcely audible with no trouble. Listening to the line signal at the transmitter end of the simulated line gave a noise signal in which no speech could be detected. The signal level was found to be of the order of 40 dB below the noise at this point. This is about 12 dBs better than the calculated figure for 3 kHz but the speech energy is weakest at this end of the spectrum so the result is substantially what would be expected.

18. A more complex form of simulation for Z_1, consisting of ten sections of 1 Ω and 0.02 pF, was tried. This gave the same results as above but needed a similar network for Z_2 to obtain good nulls of noise in V.

APPENDIX II

Analysis of the System Indicated in Figure 6

1. Figure 6 illustrates a very simple set of alternative distributions for (e_1,r_1). One is locus A in which the point lies on the line $e_1 + Ir_1 = K$, and the other is locus B, defined by $e_1 + Ir_1 = -K$. Here I and K are constants having the dimensions of current and voltage respectively. As was indicated in the section "Possibility of application to a real communication system", the sender chooses locus A or B according to the bit of information he wishes to transmit and places s_1 on it in a random manner. The recipient places s_2 somewhere in the plane and the two points define the line of Figure 5c. The recipient now calculates the probabilities of s_1 being on each locus from the information at his disposal, and, after a number of trials arrives at a reasonable certainty of which locus is being used. This is done as follows.

2. The point s_1 is known to lie on the line

$$e = e_1 - ir_1$$

and if it lies on locus A it also satisfies

$$K = e_1 + Ir_1$$

Solving these equations gives

$$r_1 = \frac{K - e}{I + i}$$

and

$$e_1 = \frac{eI + Ki}{i + I}$$

The square of the distance between s_1 and s_2 is therefore

$$\left[e_1 - e_2\right]^2 + \left[Ir_1 - I(-r_2)\right]^2 = \left(\frac{eI + Ki}{I + i} - e_2\right)^2 + I^2\left(\frac{K - e}{I + i} + r_2\right)^2$$

$$= \frac{(e + Kt - e_2 - e_2t)^2 + (K - e + r_2I + r_2It)^2}{(i + t)^2}$$

where

$$t = \frac{i}{I}$$

3. A similar result for locus B can be obtained by replacing K by $-K$ is this expression. Let the two distances be denoted by D_A and D_B respectively.

4. The probability of s_1 lying at a particular point on locus A, given that it lies on A, is proportional to the probability density at this point. Thus the probability of a line through s_1 passing through the point is proportioned to the probability density multiplied by the length of line swept by a vector through s_2 per unit angle at this point.

5. Thus the probability is proportional to $\frac{P_A D_A}{\sin \theta}$, where P_A is the probability density at the intersection of locus A and s_1 s_2, and θ is the angle of intersection between s_1 s_2 and locus A. The probability for the case of locus B is similarly proportional to

$$\frac{P_B D_B}{\sin \theta}$$

θ is, of course, the same for both loci.

6. Therefore, by Turin's theorem, the odds in favour of s_1 being on locus A are multiplied by a factor of $\frac{P_A D_A}{P_B D_B}$ compared with what they were before the trial.

7. P_A and P_B are assumed to be known to the interceptor and would take some convenient form, perhaps endeavouring to keep the ratio P_A/P_B close to unity. D_A and D_B would be calculated as above by the recipient, but the interceptor would be unable to duplicate this calculation as he would be unaware of the position of s_2.

"THE POSSIBILITY OF SECURE NON-SECRET ANALOGUE ENCRYPTION."

Z32490.

SECRET.

SHEET 1-8

COMMUNICATIONS-ELECTRONIC SECURITY GROUP

ISSUE	AMENDMENT PARTICULARS	DATE	INITIALS

R. R. 3007

DRN. J.E.L.
CKD. G.J.S.
APPD.
DATE. 31.12.69.

NOTES FOR FIGS. 1 & 2.

1. BOXES HAVE THE PROPERTIES INDICATED WITHIN THEM.
2. [N] IS A NOISE GENERATOR
3. THE SYMBOL ⊕ INDICATES A SIGNAL SUMMATION ON THE LINE ITSELF i.e. WITHOUT A BUFFER
4. Z IS THE LINE IMPEDANCE SEEN FROM THE RECEIVER.

SECRET

"THE POSSIBILITY OF SECURE NON-SECRET. ANALOGUE ENCRYPTION"

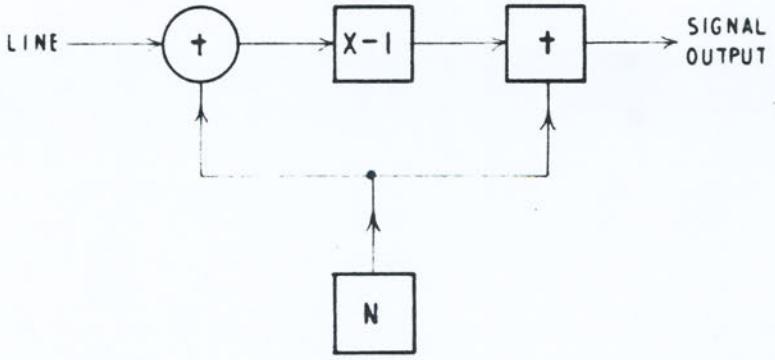
Z 32490.
SECRET.

COMMUNICATIONS-ELECTRONIC SECURITY GROUP.

ISSUE	AMENDMENT PARTICULARS	DATE	INITIALS

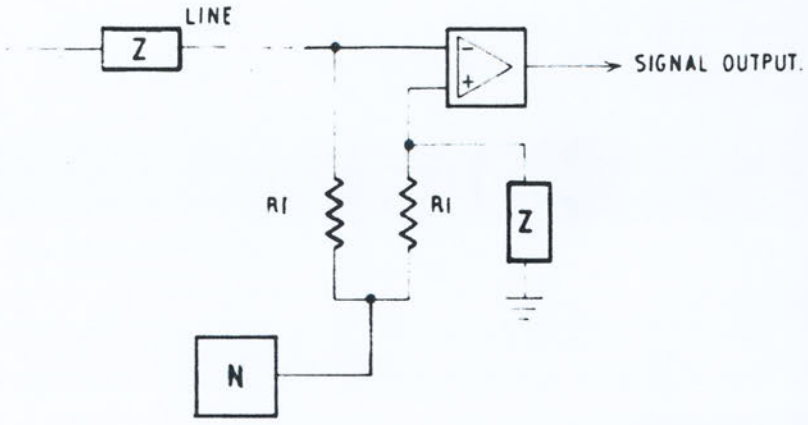
R.R. 3007.

DRN.
CKD.
APPD.
DATE.



1a

LOGIC DIAGRAM OF NOISE-ADDITIVE SYSTEM



1b

CIRCUIT SCHEMATIC OF NOISE-ADDITIVE SYSTEM

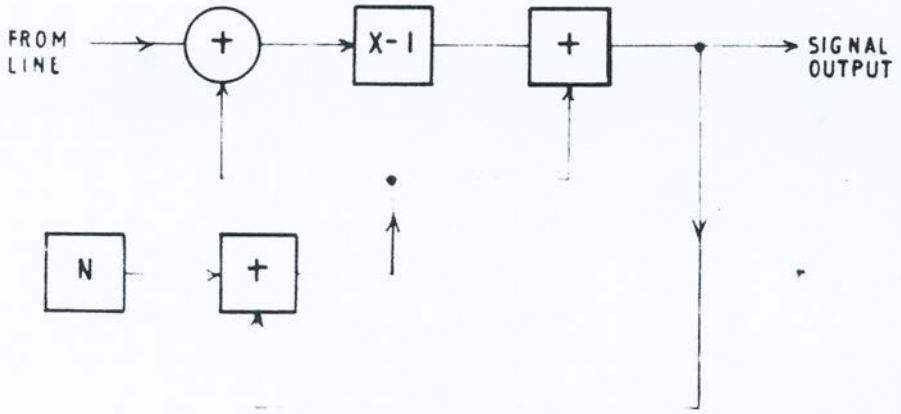
SECRET

"THE POSSIBILITY OF SECURE NON-SECRET ANALOGUE ENCRYPTION."

Z32490.
SECRET

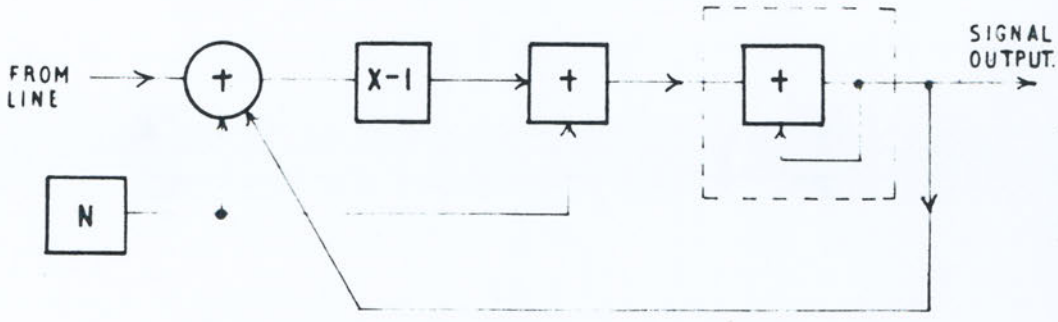
COMMUNICATIONS-ELECTRONIC SECURITY GROUP

ISSUE	AMENDMENT PARTICULARS	DATE	INITIALS



2a

SIGNAL CANCELLATION ADDED TO 1a



2b

EQUIVALENT TO 2a

R.R 3007

DRN. J.C.L.
CKD. & A.R.
APPD. J.C.L.
DATE. 31-12-69

SECRET

"THE POSSIBILITY OF SECURE NON-SECRET ANALOGUE ENCRYPTION."

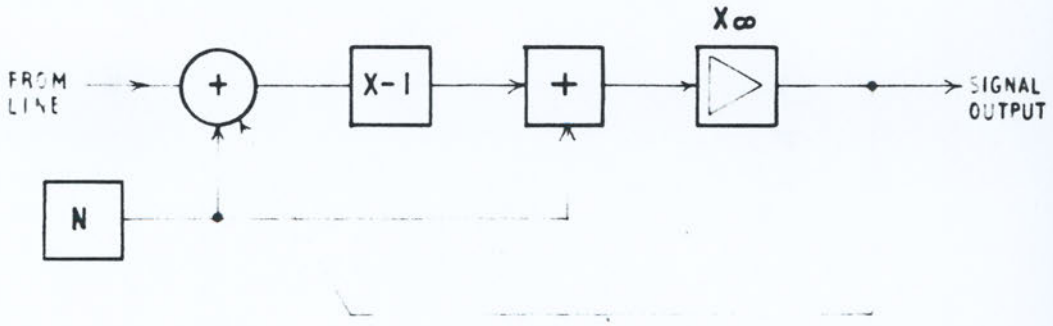
Z32490.
SECRET.

COMMUNICATIONS-ELECTRONIC SECURITY GROUP

ISSUE	AMENDMENT PARTICULARS	DATE	INITIALS

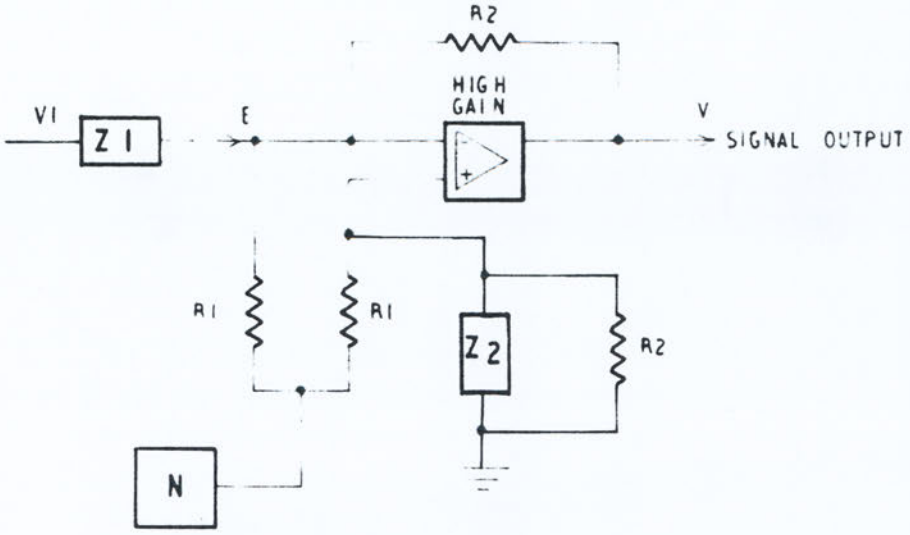
R.R. 3007.

DRN. J.C.L.
CKD. R.G.R.
APPD. G.C.
DATE. 30-12-67



2C

EQUIVALENT TO 2b.



2d

CIRCUIT SCHEMATIC OF SIGNAL-CANCELLATION SYSTEM

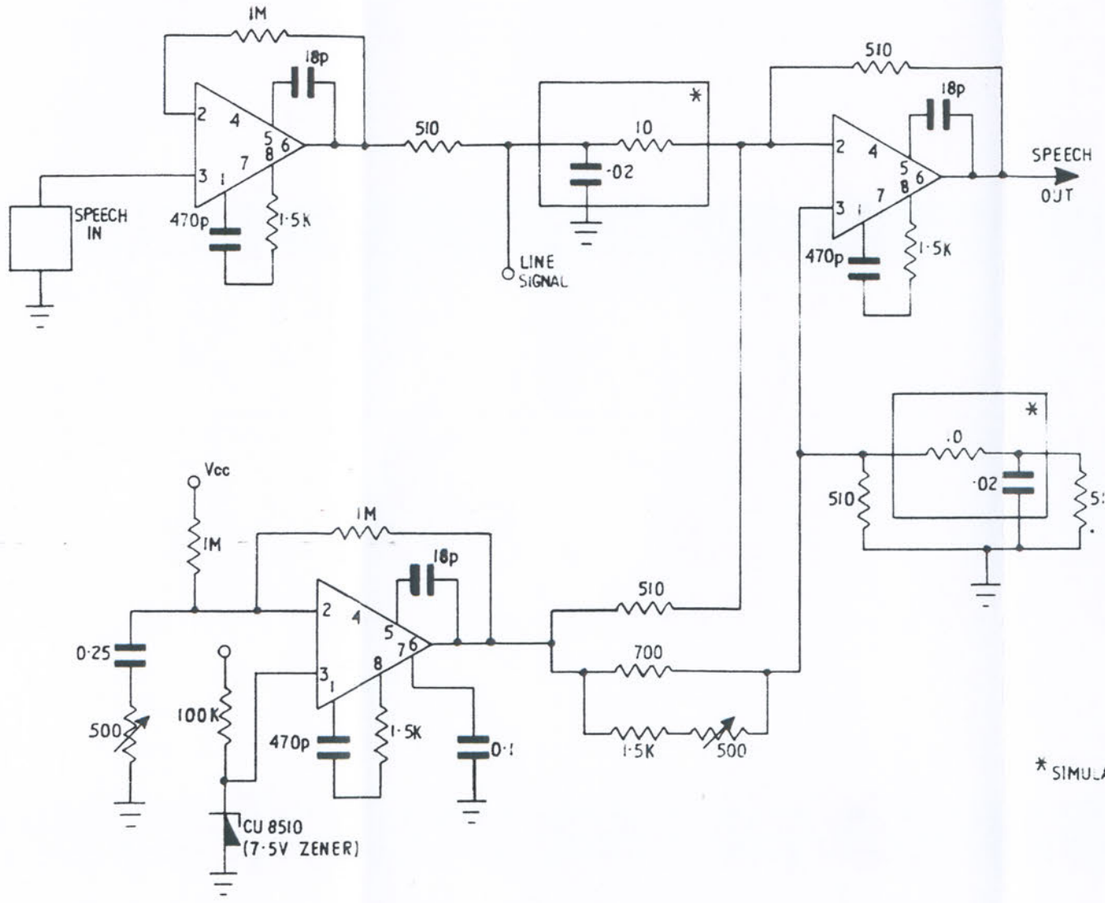
SECRET

COMMUNICATIONS-ELECTRONIC SECURITY GROUP.

ISSUE	AMENDMENT PARTICULARS	DATE	INITIALS

R. R. 3007

DRN. [illegible]
CKD. P.L.R.
APPD. [illegible]
DATE 2.12.69



* SIMULATION OF 1000Ω LINE

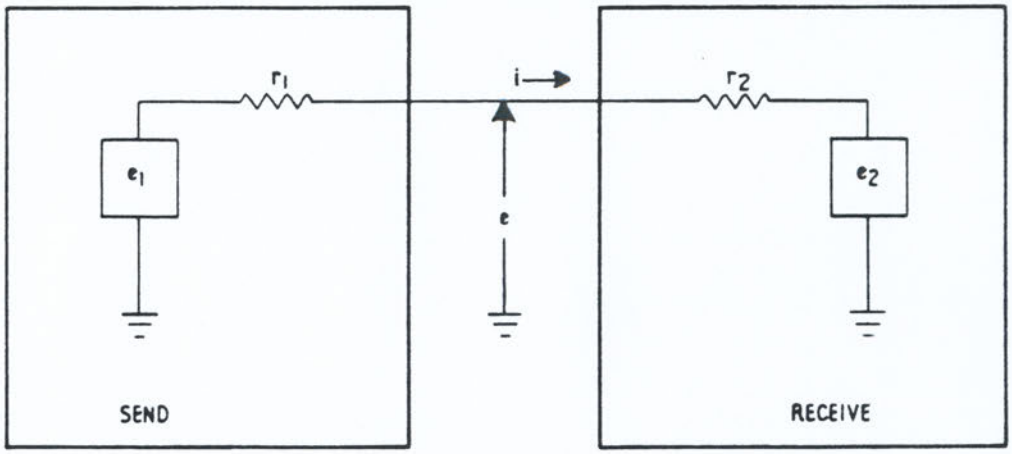
FIG.3
SIGNAL-CANCELLATION SYSTEM CIRCUIT DIAGRAM

NOTE:-
PIN 7=+15V
PIN 4=-15V
AMPLIFIERS ARE μA709.

SECRET

COMMUNICATIONS-ELECTRONIC SECURITY GROUP

ISSUE	AMENDMENT PARTICULARS	DATE	INITIALS



$e = e_1 - ir_1 = e_2 + ir_2$

FIG.4
EQUIVALENT CIRCUIT OF GENERAL COMMUNICATION SYSTEM

K R 3001

DRN.
CKD. B.A.R.
APPD.
DATE. 4 12 65

"THE POSSIBILITY OF SECURE NON-SECRET ANALOGUE ENCRYPTION."

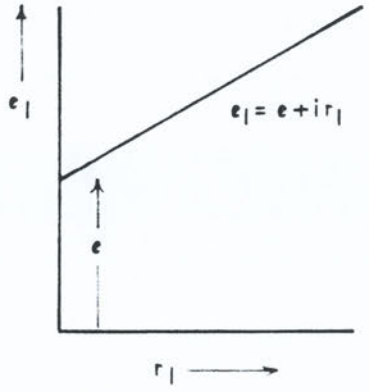
Z3249C
SECRET.
SHEET 7–8

COMMUNICATIONS-ELECTRONIC SECURITY GROUP.

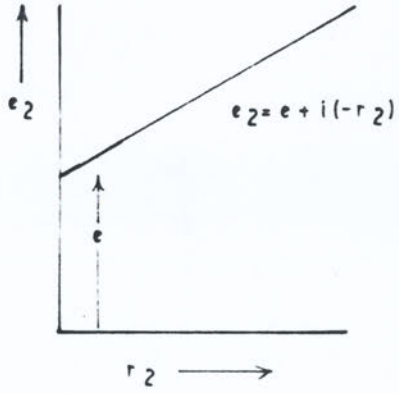
ISSUE	AMENDMENT PARTICULARS	DATE	INITIALS

R.R. 3007

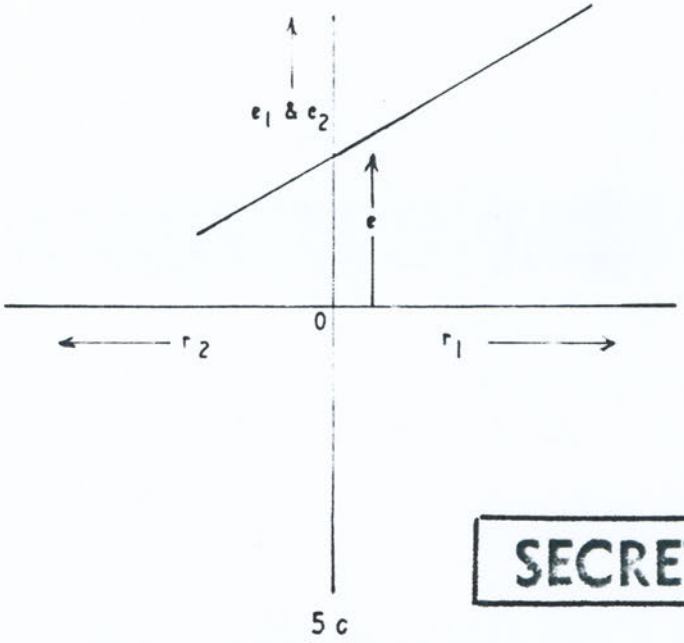
DRN. S.E.L.
CKD
APPD
DATE 31-12-69



5 a



5 b



5 c

SECRET

RELATIONSHIPS BETWEEN THE PARAMETERS OF FIG. 4.

COMMUNICATIONS-ELECTRONIC SECURITY GROUP

ISSUE	AMENDMENT PARTICULARS	DATE	INITIALS

RR 3001

DRN. JEL.
CKD. [illegible]
APPD. [illegible]
DATE. 30-12-63

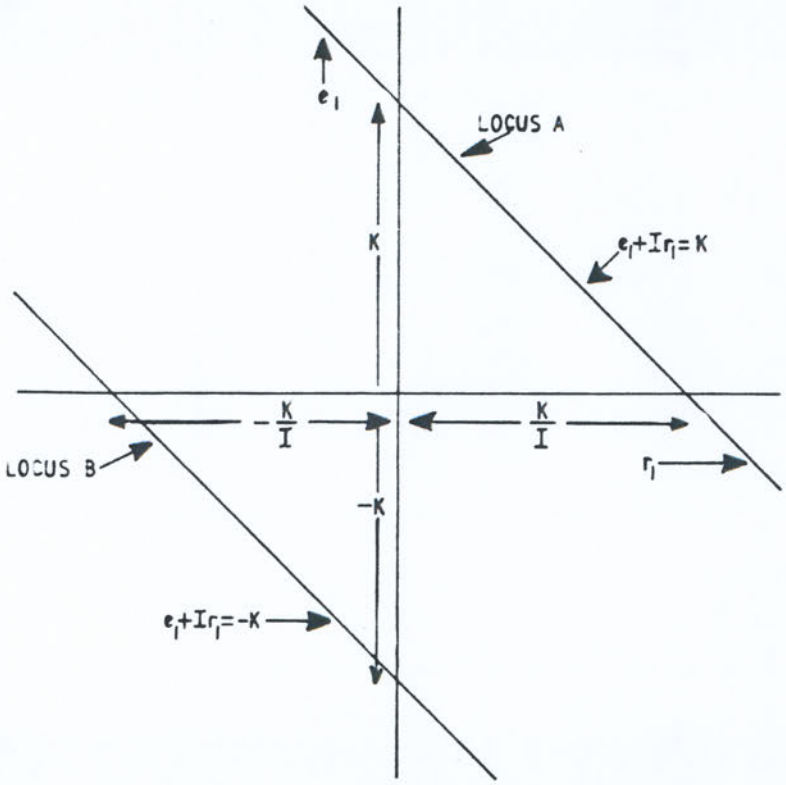


FIG. 6

ALTERNATIVE LOCI FOR (e_1, r_1)

SECRET