[redacted]

NRL REPORT R-3433

COPY NO. 44

FR-3433

[redacted]

A PROPOSED SYSTEM OF ELECTRONIC RECOGNITION

REPORT OF PROGRESS II

[redacted]

NAVAL RESEARCH LABORATORY

WASHINGTON, D.C.

[redacted]

NRL REPORT R-3433
COPY NO. 47

A PROPOSED SYSTEM OF ELECTRONIC RECOGNITION
REPORT OF PROGRESS II

C. E. Cleeton

March 16, 1949

Approved by:

Dr. J. M. Miller, Superintendent, Radio Division I

NAVAL RESEARCH LABORATORY
CAPTAIN F. R. FURTH, USN, DIRECTOR
WASHINGTON, D.C.

DISTRIBUTION

	Copy No.
BuShips Attn: Code 911 (917)	(1-10)
ONR Attn: Code 482	(11-12)
CO, ONR, Boston	(13)
CNO Attn: Op-413 Attn: Op-204D	(14-15) (16)
BuAer Attn: Aer-EL-83	(17-18)
BuOrd Attn: Re4f	(19-20)
Dir., USNEL Attn: Dr. R. O. Burns	(21-22)
Cdr., USNOTS Attn: Reports Unit	(23-24)
SNLO, USNELO	(25)
Ch., Army Security Agency	(26)
OCSigO Attn: Ch., Eng. & Tech. Div., SIGTM-S	(27)
CO, SCEL Attn: Dir. of Engineering	(28)
Dir., ESL Attn: Mr. Stokes	(29)
CG, USAF Attn: AFDRE-2F	(30)

	Copy No.
CG, AMC, Wright-Patterson Air Force Base	
Attn: MCREEC	(31)
Attn: MCREEC-53	(32)
CO, Watson Labs, Red Bank	
Attn: WLENA	(33)
CO, AMC, Cambridge Field Station, Cambridge	(34)
RDB	
Attn: Mr. S. C. Hight	(35)
Attn: Dr. L. R. Philpott	(36)
Attn: Dr. I. A. Getting	(37)
Attn: Library	(38-39)
Attn: Navy Secretary	(40)
Science and Technology Project	
Attn: Mr. J. H. Heald	(41-42)
NRL (Code 2026)	(43-100)

CONTENTS

FOREWORD

The Security Systems Section of NRL's Radio Division I has since the end of World War II been engaged largely in the development of techniques suitable for an improved system of electronic recognition, commonly known as IFF. An analysis of the problem and a progress report have previously been submitted, and a tentative system has been proposed. It is the purpose of this report to record latest developments in the over-all system as well as in the various specific techniques under investigation.

Herein described is a proposed IFF system which appears capable of preventing an enemy from deceiving us in the guise of a friend. The required security is obtained by cryptographic methods providing a very high probability that any authorized reply is generated by a friend, a condition necessary for automatic-weapon systems. For convenient reference, all related NRL reports to date have been listed in the literature cited at the end of this report.

The recently established policy for the fitting of the IFF Mark X, a system based upon the IFF Mark 5/UNB, does not materially affect the existing IFF research program. The new system described here may be considered as one to replace the IFF Mark X, and the techniques under development are largely directed toward that end although some may find application as a modification to the Mark X to improve its security or performance in other respects.

Included is a review of the status of specific auxiliary projects to develop the necessary new techniques (in transmitting and receiving equipment and in selecting and switching devices for coding and decoding) for use in the proposed system. The major problem appears to be that of reducing proposed methods to practical design.

PROBLEM STATUS

This report summarizes work on the problem to date; investigation is continuing.

AUTHORIZATION

NRL Problem No. R03-06R

A PROPOSED SYSTEM OF ELECTRONIC RECOGNITION
REPORT OF PROGRESS II

INTRODUCTION

The primary problem in electronic recognition is to devise a system which will prevent an enemy from deceiving us in the guise of a friend. At the same time there are numerous other requirements of performance which must be met if the system is to be satisfactory. For reasons of economy, advantage must be taken of the IFF equipment to supply auxiliary functions where practicable.

Some of the mystery surrounding IFF may be removed if the problem is considered merely as a two-way communication system which is required to convey two types of information, one being the position coordinates of the interrogated object, the other being the simple message, "Are you a friend?" with the reply, when given, "Yes."

Associated with the determination of position coordinates are problems of accuracy and resolution. With one exception, these are largely concerned with equipment design and are similar to those met in radar locating equipments. In an IFF system it is probably practical to measure the altitude at the transpondor location and relay the data to the interrogator. However, inability of the detection system to measure accurately the absolute altitude may limit the usefulness of altitude measurements at the transpondor.

The real problem arises in finding a means of communicating the simple message, known to enemy and friend alike, "Are you a friend?" in such a way that the enemy cannot say "Yes" to deceive the interrogator. Clearly, it is required that the reception of the authorized reply be sufficient to insure it was produced by a friend. Previous methods of recognition, including the proposed IFF Mark X, have obtained their security by a different procedure. There has never been a cryptographic encipherment of the message. The degree of security attained heretofore resulted from an operational procedure in which the IFF system furnishes information in plain text. This could be trusted only because the enemy was not expected to use like equipment or because the information was part of a composite intelligence from which recognition could be effected.

This former technique is becoming less satisfactory as the volume and complexity of necessary data increases. With the expected higher speeds of targets and with weapons automatically controlled, the IFF system must provide complete recognition of detected targets. Anything short of an immediate answer with true cryptographic security would not justify the effort to replace existing systems.

PROPOSED SYSTEM

General Type of System

The essential characteristics of the presently proposed electronic recognition system remain as previously suggested.†[8] There has been, however, a considerable improvement in details. In brief, a pulse-type interrogator-transpondor radio-frequency system is proposed, in which an enemy is recognized by eliminating friends. The latter are recognized by establishing through one or more space coordinates a one-to-one correspondence between the radar-detected target and the authorized IFF reply signal.

A coded interrogation induces a coded reply from the transpondors, and the security is obtained by varying the cross connection relationship between the interrogation and reply codes. Previously, it was considered necessary to use a chronometer-controlled device to vary this relationship frequently in a random fashion. The programming cycle would be changed whenever equipment seemed likely to fall into enemy hands. Recent developments offer encoding techniques which will relax the tolerances on the chronometer or possibly even eliminate its necessity.

Number of Interrogation Codes Required

The very nature of an IFF system makes both the plain text and encipherment immediately available to any listener. A given interrogation code, which is an encipherment of the question, "Are you a friend?" can be used once only, because an enemy could, by observation, determine the reply then authorized for saying "Yes." Further, the enemy can, by use of a captured or fabricated interrogator, cause one of our transpondors to provide the authorized reply to any interrogation. He may try all possible codes and use this information to set up a transpondor of his own to deceive us. Accordingly, we must not only arrange to pick (by a process providing no aid to prediction of future interrogation) a new code for each interrogation, but we must also have available more interrogation codes than the enemy could possibly run through rapidly enough to be of practical use.

How many interrogation codes are needed? Obviously any practical answer must be based upon certain assumptions. To obtain a perfectly safe figure, we will assume that the enemy has all possible advantages. The number will be dependent upon the rate at which the enemy could induce replies from our transpondor, the number of our transpondors available to him, and the length of time we desire a particular encoding arrangement to be secure. Now assume:

Maximum transpondor reply rate (assume enemy has use of full rate)	5000/sec.
Maximum number of transpondors available to the enemy (so separated geographically that only one enemy interrogator will trigger each transpondor)	25
Desired duration of a given encoding arrangement	24 hrs.
Time of propagation from enemy's interrogator to our transpondor (necessary assumption since enemy could devise means to avoid waiting for a reply before another interrogation was transmitted)	0
Time to record and analyze data	0.

† List of references will be found at end of report.

If it is desired that the enemy take not less than 24 hours to induce from our 25 isolated transpondors replies to all interrogation codes, then these assumptions lead to a figure of about 10^{10} as an upper limit to the number of codes needed. This order of magnitude is satisfactory for present considerations. When more is known about the technical design of equipment and the nature of future operations, a new value may be selected. To permit a material reduction in the number of interrogation codes, the major factor to be increased is the time one may safely expect the enemy to require to record and analyze the data.

Number of Reply Codes Required

The number of reply codes required is dependent upon what is considered a negligible probability of guessing the correct one. Suppose we examine the probability of guessing correctly when a total of 10 codes is available.

For any single interrogation (one code group) obviously there is one chance in ten of guessing the correct reply. As a result, however, of unavoidable transpondor count-down, fruit, and failure of signals to be received with adequate intensity, any IFF electronic system of the interrogator-responsor-transpondor type must perform some integration of the replies before identification can be positive. Regardless of whether the reply is displayed on conventional PPI's, or is electronically decoded and a locally generated signal is produced, several replies must be received to produce a discernible signal. The exact number can be predetermined in an electronic decoding system, but if directly displayed on a PPI, the number required will be a function of scope clutter, operator perception, and similar factors.

Assuming that the signals of the enemy always get through, one can compute the probability, for various specific situations, that he will give sufficient correct replies to be identified. Suppose we may expect to receive 15 pulses in each beam sweep of the antenna and that 5 or more out of the possible 15 must be correctly received to give a friendly indication. The probability of guessing 5 or more correctly out of 15 is found by summing the probability of guessing correctly exactly 5 times, exactly 6 times, and so on up to exactly 15 times. The probability that exactly n correct guesses will be made in m chances is

$$P_m(n) = C_n^m \, p^n (1 - p)^{m-n} = \frac{m!\, p^n}{n!\,(m - n)!} (1 - p)^{m-n},$$

where p is the probability of guessing correctly on any one reply (0.1 for 10 reply codes). Hence, the probability of guessing correctly exactly 5 times out of 15 chances is very nearly one in 100, that of giving the correct reply exactly 6 times out of 15 is about one in 500, and so on. Only the first term is significant, and it is seen that the probability of deception is small for this situation. Actually, in practice the enemy would have to continue to guess correctly the required percentage of the time each time he came within the sweep of the antenna, and further, he must provide his quota of correct guesses to each interrogator since no two interrogators would be expected to use the same code. Thus, the order of 10 reply codes would certainly appear to be ample.

Accomplishment

The required number of interrogation codes can readily be produced. For example if the code consisted of 10 pulses, each of which could be transmitted on any one of 10 frequencies, 10^{10} codes result. This may easily be seen if the kinds of pulses, represented by frequency, are compared to the symbols 0 to 9 used in the decimal numbering system.

The 10 pulses then correspond to a 10-digit number which could be selected anywhere between one and 10^{10} (zero replaced by ten to avoid confusion), assuming that one and only one pulse is transmitted at each time position. Should there be difficulty in the use of 10 frequencies, a system could be used permitting more than one frequency per pulse. For example, 7 kinds of pulses could be represented by only 3 frequencies, that is, A, B, C, A + B, A + C, B + C, and A + B + C. In a similar manner, 15 kinds of pulses may be produced from four frequencies.

The means of producing reply codes, on the other hand, is quite limited. Separate frequency channels must be used to designate each code if garbling is to be avoided. Garbling on the reply path with time-spaced codes occurs as a consequence of the way in which range is measured. Ten frequency channels seem reasonable to attain even though they must be selected rapidly (in a matter of microseconds). It is realized that some nonauthorized channels must be examined with each interrogation to prevent enemy deception by replying on all channels to each interrogation.

The remaining problem is that of selecting the response for each interrogation. This may be thought of as a problem of reducing a 10^{10} -character alphabet to one of 10 characters. Further, the codes must be reduced in such a way that first, there is no pattern to the association between the interrogation and reply codes and, second, that the association arrangement may be changed manually as necessary. It is desirable to determine what is required to accomplish this more or less ideally secure system. Simplification of equipment and practical problems both in our own use and in enemy countermeasures can be considered later.

In principle, decoding is carried out by considering the interrogation code as a 10-digit number and making a substitution for each digit to obtain a new 10-digit number. The substitution for any one digit will depend upon the value of all ten digits in the original number. The final digit of the new number will select directly the reply code to be transmitted.

An explanation of a suggested mechanism is provided by Figure 1. A ten-by-ten array of numbers is selected at random, except that each number from 1 to 10 (10 replaces zero) is used only once in any row or column. This array is known as a Latin Square. The kind of pulse - denoted, say, by frequencies numbered from 1 to 10 - will be used to select the order of the horizontal rows, and the order of the pulse in time will be used to denote operations.

Now, for example, suppose the first pulse of the code received occurred on channel 8 and that the first operation occurred in column 1. Referring to the array, we find that the number which is eight rows up in the first column is 5. This number will be used to select the column for the second operation, that is, column 5. If the second pulse is on channel 2, we see that 8 will be the column for the third operation, and so on. The process may be continued until we have a new ten-digit number where the digits are made up of the number assigned to the operations called for in progressing through the array. This number, however, does not have the characteristics desired, for the substitution made in each case depended only upon the preceding numbers.

Suppose the entire interrogation is delayed and sent through the array a second time, with the difference that, instead of performing the first operation in the first column, we start in the column designated by the last digit of the new number found from the first progress through the array. We obtain by substitution a second number which has the desired characteristics, and we may use the last digit of this number to select the reply. Two examples are given in Figure 1. In the first, the interrogation consists of 10 pulses,

all transmitted on frequency channel 1. After a double substitution, the last digit, 10, selects the reply channel 10. In the second example, the last pulse is varied, and the resulting change in encoding may be observed by comparison with the previous example. Obviously, possible arrangements of the array are numerous, and the one in use could be altered, say on a daily schedule, to avoid compromise either by capture or by successful analysis through interrogations and associated replies.

10	7	4	6	10	1	5	3	8	9	2
9	4	5	7	9	10	2	8	1	6	3
8	5	8	4	1	9	3	2	10	7	6
7	8	3	10	7	4	6	9	2	5	1
6	6	1	5	3	2	4	7	9	10	8
5	10	9	8	5	7	1	6	3	2	4
4	1	6	2	4	3	10	5	7	8	9
3	3	7	9	2	6	8	10	4	1	5
2	9	2	3	6	8	7	1	5	4	10
1	2	10	1	8	5	9	4	6	3	7
	1	2	3	4	5	6	7	8	9	10

start

EXAMPLES:

Input	1	1	1	1	1	1	1	1	1	1
	2	10	7	4	8	6	9	3	1	2
	10	7	4	8	6	9	3	1	2	10 → output
Input	1	1	1	1	1	1	1	1	1	2
	2	10	7	4	8	6	9	3	1	9
	3	1	2	10	7	4	8	6	9	4 → output

Fig. 1 - Encoding Array

There are numerous possibilities for design of an "electronic Latin Square" which would select the proper reply code for each interrogation. The method which, because of possible small size and low power consumption, appears most promising is a crossbar

arrangement in which selection of the horizontal conducting bar is determined by the individual received pulse and the vertical bar is energized in accordance with the interrogation code and the array in use. The points determined by the intersection of the two energized bars replaces the boxes of Figure 6. At each cross point there is a network consisting of resistors and a crystal diode; the latter acts as a switch to select the vertical bar for the next operation.

Analysis

We are concerned whether such a device will in fact provide the security indicated. In the beginning we assumed no practical limitations imposed on the enemy. He is assumed to have complete technical information on the system, even to possession of equipments, and he is not limited by facilities or techniques. His only limitation is that of the rate at which he can induce replies from our transpondors. Here we assumed he had full use of 25 transpondors capable of 5000 replies per second.

Two means of breaking the system are apparent. One is merely to find the proper reply for each interrogation by systematically interrogating our transpondors. But this we have anticipated by arranging to change the encoding system before the enemy can collect his data.

A second method would be to construct a library of all possible arrays, so indexed that a few interrogations would determine the only arrangement possible. For example, of all possible arrangements, only one-tenth of them would give a specific reply code to a given interrogation. By a proper choice of a second interrogation, the possible arrangements could be isolated to one tenth of those remaining, and so on. Though this method is possible theoretically, practical success seems doubtful because of the tremendous effort required. The number of possible Latin Squares for the case considered is unknown, but it is much larger than $10! \times 9!$, which is about 10^{12} (see Appendix). If there were only 10^{12} arrangements, and these were arranged on punched cards, it would require over a million years to run the cards through a single machine at the rate of 400 per minute.

EVALUATION OF PROPOSED SYSTEM

The proposed system appears to offer desired security against enemy deception. It has been discussed with the cryptoanalysis personnel of the Military Services. Although one can never be positive that the system cannot be broken, to date no method of analysis has been discovered which would appear practical.

There has been no advance in methods for preventing unauthorized interrogation, but this aspect of security is considered second in importance to that of preventing an enemy from deceiving us so as to appear as a friend.

Traffic on the reply path, the limiting path in previous systems, is divided among the reply frequency channels (10 suggested).

Estimation of the ability of the system to perform auxiliary functions is held in abeyance until more practical devices are developed to perform the primary functions of IFF. There is a reasonable expectation that really essential functions can be incorporated into the final equipment, though certainly not without additional complication.

It is assumed that any future equipment will make the fullest use of the art in reliability and miniaturization of components and anti-jam circuits.

PROGRESS ON TECHNIQUES

Specific projects required to carry out the proposed program are listed in this section with information as to their status. Included are projects not specifically required for the proposed system but which form a part of the program on development of new techniques and collection of information. Numerous related projects have been reported in detail (and a supplementary bibliography has been included with the list of references cited).

Electronic Tuning

A transmitter tube, suitable for airborne transpondor use, is required which can be tuned electronically to any one of about 10 channels in a manner of a few microseconds after decoding of the interrogation signal.

An experimental magnetron is being developed by Raytheon under a Bureau of Ships contract for this use. The Naval Research Laboratory has experimented with the QK151 which was originally designed as a 50-watt C.W. magnetron for frequency modulation up to about 12 Mc at a center frequency of 3800 Mc. Under pulsed conditions, an efficiency of about 25 percent has been obtained over an electronically tuned range of 30 Mc with one tube. Although considerable thought has been given to electronic tuning of conventional tubes, no suitable techniques have been devised.

Cryptographic Encoding

A device is required which will select a reply code dependent upon the interrogation code. The inter-relationships between the interrogation and reply codes must follow no pattern and must be capable of at least daily rearrangement.

Numerous possible methods have been considered, such as electron beam switches, photoelectric devices, and crossbar arrays. It now appears that the most promising is a crossbar arrangement using crystal diodes in a resistor network for the selecting and switching functions. Further investigation of design requirements for such a device is being continued.

Random Code Selection

It is required to select the interrogation code in such a way that the code transmitted bears no relation to codes used previously. Also, any code should be equally probable. The time available for performing each selection would be approximately the repetition period of the interrogator.

No work has been inititated on this project.

Chronometer Control of Code Change

Initially it was considered necessary to make a change in the encoding arrangement more often than would be possible by manual means. It now appears that the frequency of such changes can be reduced because of the possibility of providing a much larger number of codes. The chronometer will be required only if it is impractical to provide equipment giving security for a period of perhaps 24 hours without mechanical change.

There is very little knowledge as to how the time-keeping qualities of chronometers are affected by such things as temperature, pressure, and vibration. A study was inititated

of standard Navy chronometers to determine what could be accomplished with chronometer-control of code change. To date all effort has been directed toward establishing controlled test conditions and devising appropriate measuring equipment.

Adjacent Channel Rejection

In the proposed system, the code character is dependent upon the presence of a signal in one or more radio frequency channels and the absence of signals in other channels. The adjacent-channel rejection must be very good if coding errors are to be avoided. Close spacing of channels is desired to conserve spectrum and to lessen the technical difficulties in tuning the transpondor transmitter electronically.

An extended investigation of discrimination circuits has been initiated. Use of the "McKinley Circuit," employing a wide band and a narrower band-detector circuit with separate detectors connected in opposition, shows considerable promise.

Defruiting

All IFF systems suffer from an excess of unsynchronized signals from interrogations by other installations. These signals are termed "fruit" and their elimination is called "defruiting."

An experimental defruiting system using the mercury delay line as the memory device was satisfactorily tested during the trials of IFF Mark V by OpDevFor.[12] Studies on storage-tube techniques for defruiting continue. An experimental system is under construction.

Circularly Polarized Radiation

Theoretically, some possibilities exist for reducing the amplitude of IFF signals arising from reflections (from objects such as ships) when circularly polarized antennas are used.

Equipment is being assembled to measure reflections from ships when circularly polarized waves are used.

Artificial Means of Improving Azimuth Discrimination

A study [2] of the problem of selecting an optimum frequency for IFF has indicated it may be impractical to build directional antennas large enough to give the desired azimuth discrimination for future high-resolution radars.

Means for reducing the arc over which interrogation occurs has been under investigation for some time. Several reports[1,9,11,13] have been distributed on antenna design. An experimental tube[14] has been constructed which will switch the interrogator power between two antenna elements during the interrogation code.

Omni-Channel Receivers

In the proposed IFF system, it will be necessary to receive signals of different radio-frequency channels simultaneously.

The use of multiple local oscillators an/or i-f amplifiers is being investigated with the view of reducing the components required and of eliminating interference between receiving components.

Video Mixing

IFF data must eventually be mixed with radar data for coordinate comparison and presentation. To obtain flexibility in use of the data, complicated interconnection equipment has always been required.

Investigations are being made of means to simplify such circuits. Experimental equipments are being constructed which utilize crystal diodes, where possible, instead of vacuum tubes. It is hoped to obtain some practical experience with such circuits with IFF Mark X installations.

ACKNOWLEDGMENT

This report of progress covers the major effort of the Security Systems Section. Appreciation is expressed to all members of the Section for their contribution in developing the techniques which comprise the proposal.

* * *

APPENDIX

The Latin Square

Enumeration of the arrangements of the Latin Square has been treated previously by MacMahon ("Combinatory Analysis," Vol. I, Chapter III. Cambridge University Press, 1915), and it has been shown that the number of Latin Squares of order n is

$$N\, n\,!(n-1)\,!$$

where N is the number of reduced Latin Squares.

A method of enumerating the number of squares is available. If the symmetric function

$$\sum a_1^{2^{n-1}} a_2^{2^{n-2}} \ldots a_{n-1}^{2} a_n$$

is raised to the power n, then the common coefficient K of the term

$$K \sum a_1^{2^n-1} a_2^{2^n-1} \ldots a_{n-1}^{2^n-1} a_n^{2^n-1}$$

is the number $N\, n\,!(n-1)!$

The enumeration has been carried out to order 5 giving the following results:

n	N	N n!(n - 1)!
2	1	2
3	1	12
4	4	576
5	56	161,280

* * *

† 6 373,248,000
† 7 61,428,210,278,400 } *

* M.G. Kendall, "The Advanced Theory of Statistics Vol II p. 259

† R.A. Fisher & F. Yates, "The 6 x 6 Latin Squares" Proc Camb. Phil. Soc. XXX 492-507

† H.W. Norton "The 7x7 Squares" Annals of Eugenics ix 269-307

REFERENCES

(Arranged chronologically. Starred (*) items are those cited in the text; others are included here as additional bibliography.)

*[1] Parker, C. V. and L. L. Cazenavette, "An Artificial Means of Improving the Azimuth Discrimination of IFF Systems," NRL Report R-2871, 13 June 1946 (Secret)

*[2] Schwartz, L. S., "Factors Affecting Choice of Operating Frequency for Electronic Recognition and Identification Systems, " NRL Report R-2906, 16 July 1946 (Secret)

[3] Cleeton, C. E., "Coding and Security of Electronic Recognition and Identification Systems," NRL Report R-2972, 12 September 1946 (Secret)

[4] Furlow, W. M., Jr. and W. L. Bulger, Jr., "A Method of Coding and Displaying IFF Reply Symbols," NRL Report R-2980, 17 December 1946 (Secret)

[5] Birnbaum, M., "Paired-Pulse Decoders Providing Echo Suppression," NRL Report R-3080, March 1947 (Confidential)

[6] Schwartz, L. S., "Statistical Methods in the Design and Development of Electronic Systems," NRL Report R-3111, July 1947 (Unclassified)

[7] Schwartz, L. S., "The Problem of Emission Interference in Electronic Recognition and Identification Systems," NRL Report R-3117, May 1947 (Secret)

*[8] Cleeton, C. E., "Proposed System of Electronic Recognition," NRL Report R-3131, June 1947 (Secret)

*[9] Parker, C. V., "Some Theoretical Considerations in the Design of Directional-Null-Type Antennas," NRL Report R-3162, 1 August 1947 (Unclassified)

[10] Schwartz, L. S., "The Attainment of Security in IFF," NRL Report R-3170, August 1947 (Secret)

*[11] Parker, C. V., "Characteristics of Directional-Null Antenna Patterns Produced by Multi-Element Arrays," NRL Report R-3245, 1 March 1948 (Unclassified)

*[12] Parsons, J. R., "IFF System Defruiting with a Mercury Delay Line," NRL Report R-3278, April 1948 (Confidential)

*[13] Fales, D., III, "Design of a Beam-Sharpening IFF Antenna for Airborne Radar," NRL Report R-3279, 14 April 1948 (Secret)

*[14] Flarity, W. H., "Development of Electron Tube for Switching Radio Frequency Power," NRL Report R-3305, 23 June 1948 (Confidential)

[15] Paull, S., "Overinterrogation and Asynchronous Replies and their Relation to Display Limitation and Traffic Handling Capacity in an IFF System," NRL Report R-3338, 25 August 1948 (Secret)