NSA

~~TOP SECRET~~ ~~EIDER~~

~~TO BE HANDLED IN ACCORDANCE WITH IRSIG~~

UKUSA C/S 651.

[redacted] ~~No. 97~~

Date: 23rd February, 1955

Copy No.: 21

PL 86-36/50 USC 3605

COMMENTS ON AFSAY D802

By Mr. [redacted]

Summary

This paper describes the AFSAY D802, discusses certain features of it and suggests two possible attacks. The validity of the attacks depends on the extent to which the output of the deltamodulator can be cribbed, exactly or statistically.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted] No. 97

Distribution

Standard.

~~TOP SECRET~~ ~~EIDER~~

~~TOP SECRET~~ ~~EIDER~~

~~TO BE HANDLED IN ACCORDANCE WITH IRSIG~~

COMMENTS ON AFSAY D802

By Mr. [redacted]

EO 3.3(h)(2)
PL 86-36/50 USC 3605

PL 86-36/50 USC 3605

References.

1. Tentative Cryptosecurity Evaluation of ASAY-4 (X-2) by [redacted] BRUSA C/S 146, April 28th 1952.

2. ASAY 4 (X-2) Low Echelon Ground Ciphony System. BRUSA C/S 201. May 7th 1952.

3. DEY 804 by [redacted] and [redacted] [redacted] No. 49. October 13th 1952.

4. Tentative Cryptosecurity Evaluation of the Alternate Cryptosysten for the AFSAY D801. Issued by NSA 412B-1. January 20th 1953.

5. U.S. Communication Security Equipments BRUSA C/S 237. August 1953.

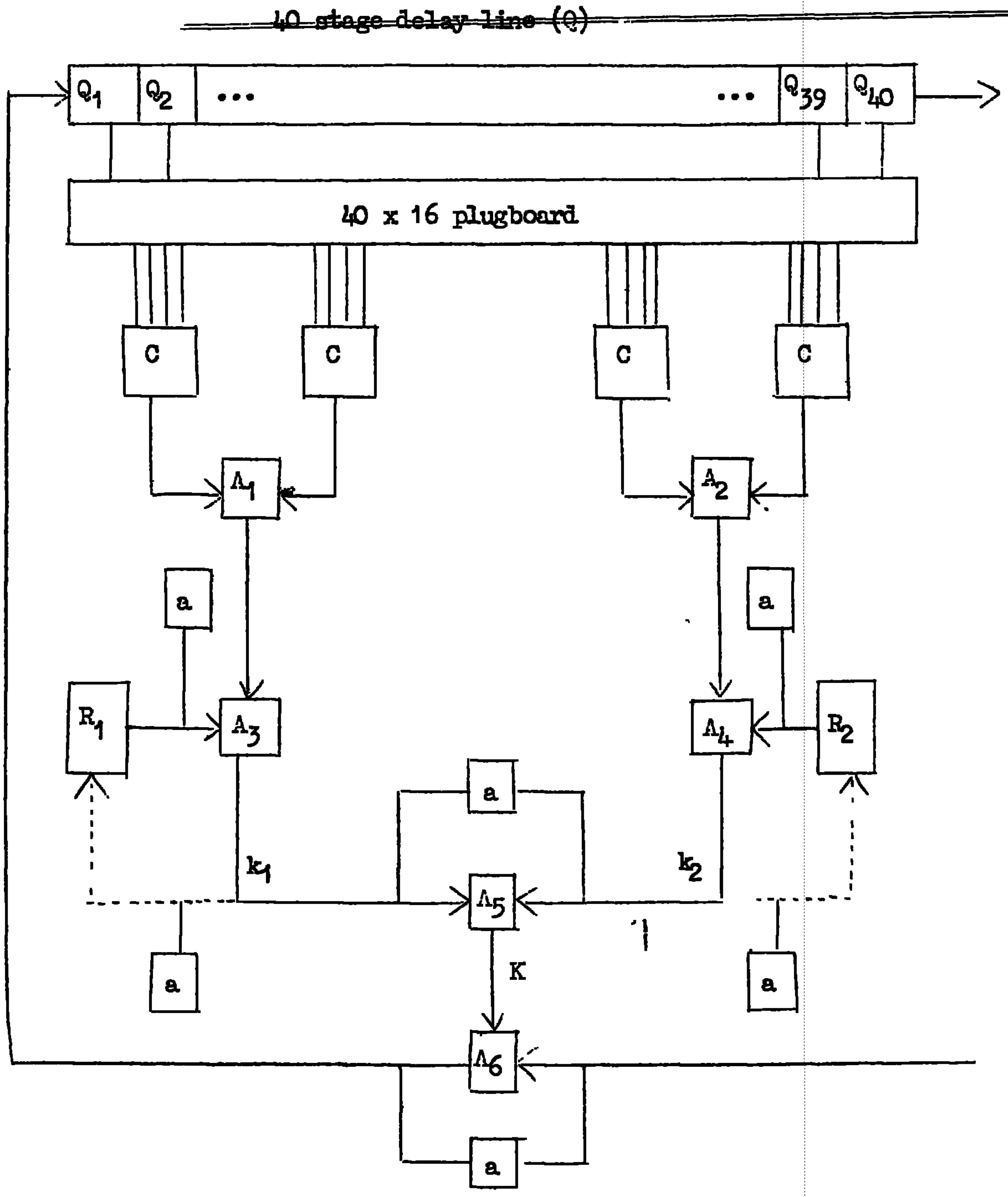
~~TOP SECRET~~

~~TO BE HANDLED IN ACCORDANCE WITH IRSIG~~

EIDER

2.

No. 97



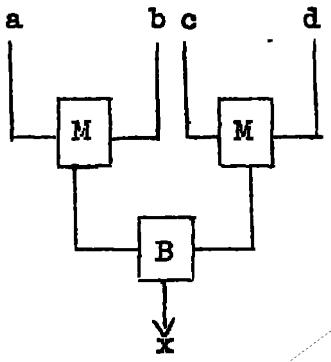
A = mod 2 addition

R = 16-longrandom walk ring

a = alarm circuit

C = Converter

Each converter is of the form



where M = multiplication and B = Boolean addition, i.e. x = ab + cd +

~~TOP SECRET~~

EIDER

Figure 2.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

No.97

AFSAY D802

1. Introduction

(a) AFSAY D804 (formerly known as ASAY 4 and DEY 804), is a low echelon speech secrecy device. It was designed and assessed in refs 1, 2 and 3, and it was concluded that the design offered only a low degree of security. A modification to this machine, known as AFSAY D802 (formerly AFSAY D804 (X-4)) is described and assessed in ref.4. This modification is designed for telephone circuits where a high degree of security is required. It is understood to be in use in small numbers, and will eventually be replaced by AFSAY D801.

(b) This paper describes the machine, discusses certain features of it and suggests some possible lines of attack.

2. Brief Description

(a) The equipment is "push-to-talk". Speech is encoded on a delta-modulator at 25 kcs. A certain amount of random noise is fed into the system. The method of encipherment is similar to that of other cipher text autokey systems, and Figure I should be for the most part self-explanatory. The main novel feature is the random walk rings R_1 and R_2. R_1 consists of the pattern 111100100011001O, and steps one position if sub-key k_1 is $\underline{1}$; if k_1 is Ø it stands. R_2 is driven similarly by k_2 and consists of the pattern 1111001101000100. In an obvious notation, K_{41} is derived from $Z_1 \dots Z_{40}$ and is added to P_{41} to produce Z_{41}.

(b) The plugboard is such that adjacent points in the delay line Q cannot be multiplied together.

(c) The alarms are understood to be as follows:-

(i) A_5 and A_6 (see Figure 1) are duplicated.

(ii) Counters count the distance between the configuration 11 in the inputs and outputs of R_1 and R_2. If this exceeds 80 elements, transmission is cut off for 300 elements, so that if the condition persists there is a nasty buzz at both the send and receive end. This guards against failure of R_1 or R_2, constant output from A_1 or A_2 and constant Ø output from A_3 or A_4, but not apparently against constant 1 output from A_3 or A_4.

(d) The first few hundred elements of each transmission are not transmitted (the paradox seems to be unavoidable).

3. Notations

The following notations are used in this paper.

Q The 40-long delay line.

Q_i The ith stage in Q.

Q' The last plugged stage in Q.

f The distance between Q' and Q_{40}, i.e. $Q' = Q_{40-f}$. If the plugging is random the median value of f is 1 and the average value 1.42.

Q'' The first plugged stage in Q.

R' The ring which Q' helps to drive.

R" The ring which Q'' helps to drive.

S Denotes 'same', when we are comparing any two elements of the enciphering process at different positions of the text.

D Denotes 'different'.

P, K and Z bear their usual meanings of plain, key and cipher.

4. Synchronisation

After 40 bits of cipher text have been transmitted Q in the receiving equipment will be identical with that in the send equipment. The expected time of coalescence of both the random walk rings can be obtained by setting $F(t) = 1 - \frac{1}{\sqrt{2}}$ in the formula of [redacted] No. 36 Appendix I paragraph 6; this evaluates to approximately 99.6 positions. The expected total time for coalescence is therefore $40 - f + 99.6 \doteq 138$ positions. This has ignored the fact that one ring can begin to coalesce one or two or so positions (according to the plugging) before the other can.

5. Key

The key is flat by monobits but has a slightly rough delta at distance one; at higher distances the bulge decreases. See paragraph 11(c) for details.

It is conceivable that the delta properties may also be affected by particular pluggings; no work has been done to confirm this.

[redacted]

7. Coalescence

(a) With suitable P/L repeats the probability of two stretches of cipher text coalescing at a given position so as to form a causal cipher repeat seems to be approximately 2^{-48+f}.

(b) The actual process of coalescence is complex, as can be seen from the following table. Immediately before coalescence occurs either Q may be D (all previous stages are S), or R' may be offset by one position either way (denote this by saying that R' is D) or both may be D, and in each case P may be either S or D. The result of such a state may either be

(i) that both Z (i.e. Q) and R' coalesce, or

(ii) that Z (i.e. Q) coalesces but R' does not or

(iii) that Z (i.e. Q) completely diverges.

Comparison of two positions in the cipher text. Q is S up to but not including Q . R' is either in phase (S) or offset one (D). The other ring is S.				Probabilities of results		
State	Condition of P/L	Q'	R'	(i) coalescence	(ii) partial coalescence	(iii) divergence
I	S	S	D	0	½	½
II	S	D	S	5/8	0	3/8
III	S	D	D	0	½	½
IV	D	S	D	1/4	1/4	½
V	D	D	S	0	3/8	5/8
VI	D	D	D	1/4	1/4	½

(c) Result (ii) from states I, III and V will leave R' at an offset of one, i.e. at the next position of text we shall have state I or IV. Result (ii) from states IV and VI will leave R' at an offset of two, which implies that if the P/L is D for the next two positions there is a 1/16 chance of Q and R' coalescing; other ways of coalescing from such a state are of course possible but are less likely and would take longer.

[redacted]

into a causal repeat.

(b) Once set-up, such repeats will only end when the P/L diverges. For the attack to progress any further we now need some knowledge of the P/L. It is not necessary to crib the two texts of a repeat but we must know whether the respective P bits are S or D in the positions succeeding the end of it. Let us assume that most or all such repeats end as follows:-

P_1.... 0 1 0 1 0 1 0 1 0 1 0 1 ......

P_2.... 0 1 0 1 0 1 1 0 1 0 1 0 ......

.... S S S S S S D D D D D D ......

(c) If the repeat ends at time 1, we shall have D at Q_1 at time 2. If Q_1 is not plugged K will be S in all cases and we can go on to time 3, 4 etc. until we find 'Q". Now let us examine all pairs of positions where there is D at "Q" and S at all subsequent stages. At 3/8 of these pairs K will be D. Examination of these pairs where K is D will immediately identify the other 3 stages plugged to the converter to which "Q" is plugged.

(d) We now take the 5/8 x 1780 pairs where K is S and repeat the process on the second plugged stage in Q using only those pairs where the alignment of R" has not been affected by D at Q", and so on.

(e) With luck we can recover most of the plugging. In a less favourable case and with less than perfect knowledge of the P/L we should get some way. If the machine has been partially solved the amount of further work required is indicated below.

Number of converters solved	Approximate ave age number of distinct pluggings still to be tested
0	[redacted]
1	$10^{14.7}$
2	$10^{9.7}$
3	$10^{4.8}$

These figures give the order of reduction obtained. In practice secondary attacks would not assume all the remaining pluggings simultaneously.

(f) It is less easy to apply this attack to the beginning of repeats because of the random walk rings. However, it will be seen from the table in paragraph 7(b) that coalescence will either arise from states IV or VI at the very beginning of a P/L repeat or will arise from state II in the middle of such a repeat. If there is much silence the second method is more likely. In this case we shall have a large number of situations analogous to the end-of-repeat situations discussed above, and the same sort of attack will appply.

(g) The WF consists mainly of the initial sort for causal cipher repeats, and, since 10^9 is an outside estimate of the number of bits required, will be less than about $10^9 (\log_2 10^9 -1) = 10^{10.46}$ sorting operations.

9. Statistical Attacks

(a) These require statistical cribbing of the delta of the plain text at distance one. It does not matter whether the cribbed bits are consecutive or not. The number of assumptions required depends on the amount of crib available. Note A describes two attacks:

Amount of exact delta crib needed	Work Factor
$10^{8.29}$ bits = 129 minutes' transmission	$10^{10.8}$ operations
$10^{5.16}$ bits = 5.7 seconds' transmission	$10^{13.9}$ operations

These are the outside figures. Others can be suitably interpolated between them.

(b) If the available crib is not exact but statistical more text is needed and the WF is correspondingly larger. See paragraph 14 for a general discussion of cribbing for these attacks.

(c) The statistical attacks are only possible because the random walk rings step "0 and 1". If it was impossible for them to hesitate - if they stepped "1 and 2" for instance - the attacks would be completely blocked.

10. Summary

This paper has considered, somewhat academically, two attacks. Both depend for their effectiveness on the properties of the plain text.

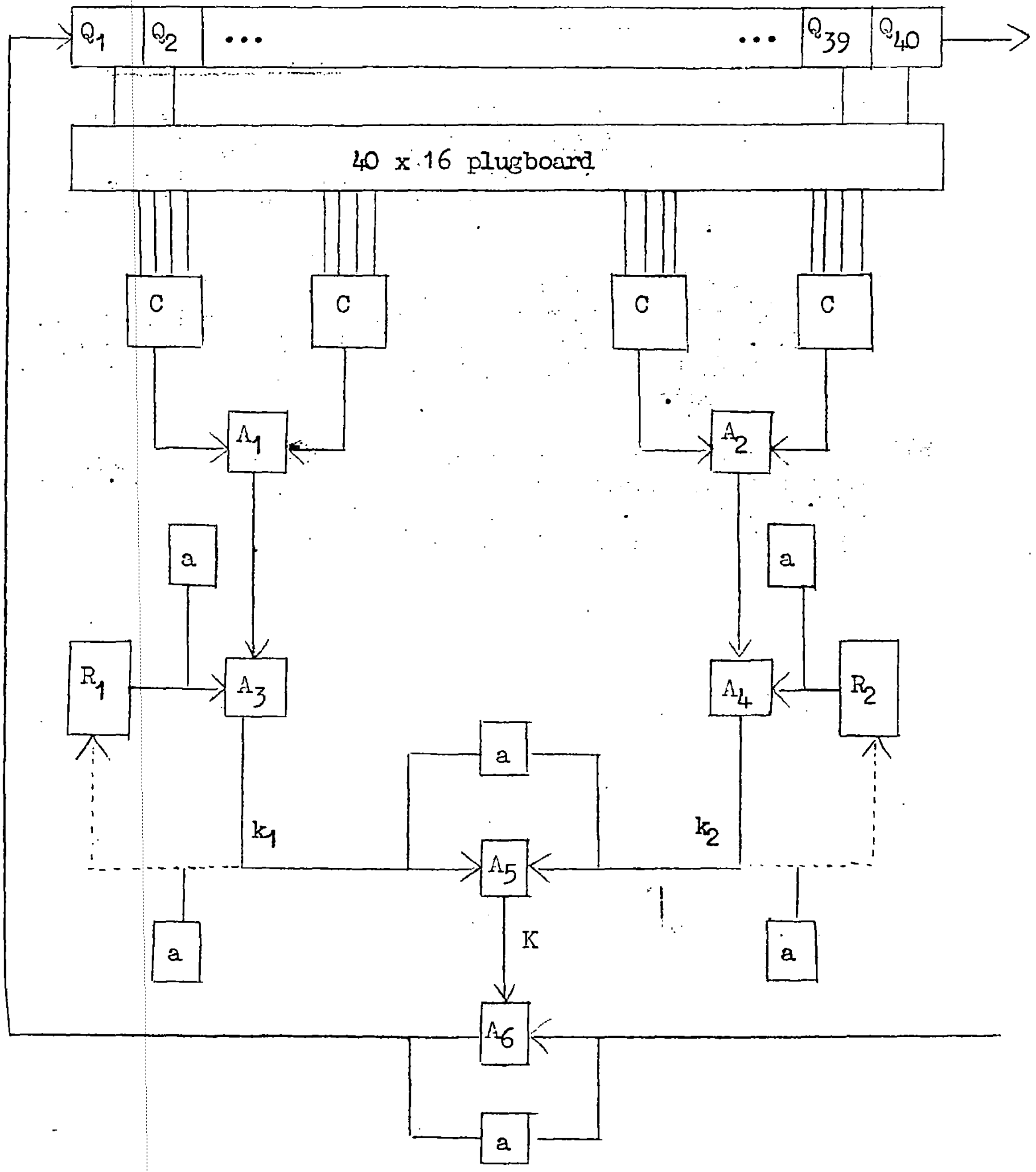
[redacted]

[redacted] No. 97

[redacted]

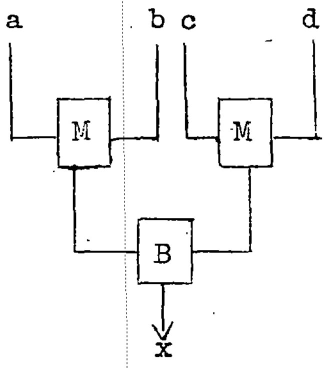
EO 3.3(h)(2)
PL 86-36/50 USC 3605

40 stage delay line (Q)



A = mod 2 addition
R = 16-longrandom walk ring
a = alarm circuit
C = Converter

Each converter is of the form



where M = multiplication and B = Boolean addition, i.e. $x = ab + cd + abcd$ (Mod 2).

Figure I

NOTE A

STATISTICAL ATTACKS

11. Properties of the Combining System (see Figure 1)

(a) The converters

(i) If a is ∅, $p(a = x) = \frac{1}{2}(1 + \frac{1}{2})$

If a is 1, $p(a = x) = \frac{1}{2}(1 + 1/4)$

where p(H) is the probability that H is true.

Similarly for b, c and d.

The average probability therefore is

$p(a = x) = \frac{1}{2}(1 + 3/8)$.

(ii) If $a = b = ab = 1$, $p(ab = x) = \frac{1}{2}(1+\frac{3}{4})$

if $ab = ∅$, $p(ab = x) = \frac{1}{2}(1 + \frac{1}{2})$

Similarly for the pair c,d.

The average probability therefore is

$p(ab = x) = \frac{1}{2}(1 + 5/8)$.

(iii) If $a = c = ∅$ $p(ac = x) = \frac{1}{2}(1 + 1)$

If $a = c = 1$, $p(ac = x) = \frac{1}{2}(1 + \frac{1}{2})$

If $a + c = 1$, $p(ac = x) = \frac{1}{2}(1 + 0)$

Similarly for the pairs a,d; b,c; b,d,
The average probability therefore is $\frac{1}{2}(1+3/8)$.

(iv) if one input to a converter is recovered the probability that the output remains unchanged is $\frac{1}{2}(1 + 1/4)$

(b) The random walk rings

If r_i is the output of a ring at time i,

$p(r_i = r_{i+1}) = \frac{1}{2}(1 + \frac{1}{2})$

$p(r_i = r_{i+2}) = 1/4 + \frac{1}{2} . \frac{1}{2} + 1/4. 3/8 = \frac{1}{2}(1 + 3/16)$

(c) The key

The final key is flat by monobits. However since for each

NOTE A

converter $p(x = \emptyset) = \frac{1}{2}(1 + \frac{1}{8})$,

$$p(K_i = K_{1 + 1}) = \frac{1}{2}(1 + (\frac{1}{8})^8 (\frac{1}{2})^2) = \frac{1}{2}(1 + 10^{-7.83})$$

and $p(K_i = K_{i + 2}) = \frac{1}{2}(1 + (\frac{1}{8})^8 (\frac{3}{16})^2) = \frac{1}{2}(1 + 10^{-8.71})$

[redacted]

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted] No. 97

[redacted]

[redacted] No. 97

[redacted]

EO 3.3(h)(2)
PL 86-36/50 USC 3605

16. Other methods

(a) The foregoing has described only 2 particular attacks, where 4 and 8 points are assumed respectively. It is of course equally valid to assume 5, 6 or 7 points, according to the amount of crib available on a given day. Unless crib is very hard to come by, it is probably not economical to assume a 3rd input to a converter.

(b) In paragraphs 12 and 13 we required sufficient text each time to prove or disprove each plugging assumption. We could alternatively have run all plugging assumptions through a shorter stretch of text, and combined the answers. This method would incidentally recover the whole plugging at one go.