(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 095 923**
A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **83303100.8**

(22) Date of filing: **31.05.83**

(51) Int. Cl.³: **H 04 K 1/06**

(30) Priority: **02.06.82 GB 8216137**

(43) Date of publication of application: **07.12.83 Bulletin 83/49**

(84) Designated Contracting States: **AT BE CH DE FR GB IT LI LU NL SE**

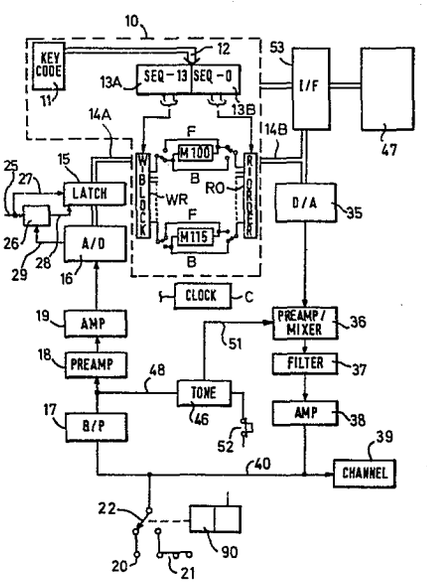
(71) Applicant: **Advance Electronic Products Limited, The Innovation Centre, Mount Pleasant Liverpool (GB)**

(72) Inventor: **Austin, Kenneth, 14 Aster Crescent, Beechwood Runcorn (GB)**

(74) Representative: **Dodd, David Michael et al, ROYSTONS 531 Tower Building Water Street, Liverpool L3 1BA (GB)**

(54) Communications scrambling systems.

(57) Scrambled communications signalling uses signals as transmitted and received that are coded by reorganisation of binary words representing original information signals. That reorganisation not only produces different sequences of blocks of binary words but also provides for variation of the lengths and numbers of such blocks (via memori M100-M115) within each reorganisation. In addition the blocks are read out in reverse order to their storage, and the preferred organisation is via a logic type pseudo random generator that must be synchronised and «seeded» at both transmitter and receiver prior to any transmission.



EP 0 095 923 A2

Title: Communications Scrambling Systems

DESCRIPTION

The invention relates to scrambled communication utilising coded electrical signals such signals normally, but not necessarily, being of analogue type as transmitted but with digitisation and reorganisation before transmission and after reception.

We are primarily interested in voice signals but do not rule out application of this invention to other analogue signals, even directly to digital signals. We find that digitisation by amplitude according to a plurality of levels to generate corresponding binary words is particularly convenient for storage and organisation purposes, especially compared with so-called bucket-brigade scrambling systems having a fixed number of input samples/components with a corresponding quite low fixed maximum number of secure scrambled reorganisations.

The invention has particular envisaged application to communications involving voice signals, whether by radiom for example the so-called "citizens band" systems, or by telephone, or otherwise.

Accordingly, we now propose scrambled communications signalling wherein signals as transmitted and received are in a coded form wherein components thereof comprising or corresponding (if analogue) to binary words comprise coded reorganisation of original or corresponding (if analogue) binary words according to sequentially different organisations which organisations comprise variable lengths (numbers of binary words) and numbers of blocks of said binary words in variable sequences different from original information order so that said signals are time-different from said original signals.

We find that a significant variable number of blocks, say variable from 8 to 16, in each organisation and a significant variable number of binary words in each block, say variable from 256 to 512, gives particularly secure scrambling, say using pseudo-random controlled sequential organisations with a very long if not effectively unrealisable repetition. Effectively, eaves-droppers cannot achieve decoding even by entering a correct key for starting coding operations after a communication is in progress as there is no clue as to block lengths or block transitions even if such have a repetitive, cyclic sequence though operation is, further preferably based on logic type pseudo random number generators.

A preferred system is operative relative to storage means for the binary words in blocks read out from storage in a sequence different from sampling order. A plurality of stores may be used, one for each possible block and each usable up to a maximum capacity corresponding to maximum block size. Alternatively, an effectively continuous memory space may be variably partitioned into blocks, if desired retaining the same total number of words in each block arrangement or sequence. It is further preferred that at least some reading out be done in reverse order advantageously to reduce residual intelligibility and add to overall security.

Even a cyclic sequence of such block definitions, say from stored random numbers, would be virtually impossible to decode except by a receiver started at the same time as the transmitter. However, a psuedo random basis of operation without repetition is preferred.

Moreover, each random number determination of number of blocks, of block size and of sequence of read-out is preferably accompanied by a following determination relative the complement of such random number(s), so that determination effectively proceeds in pairs of

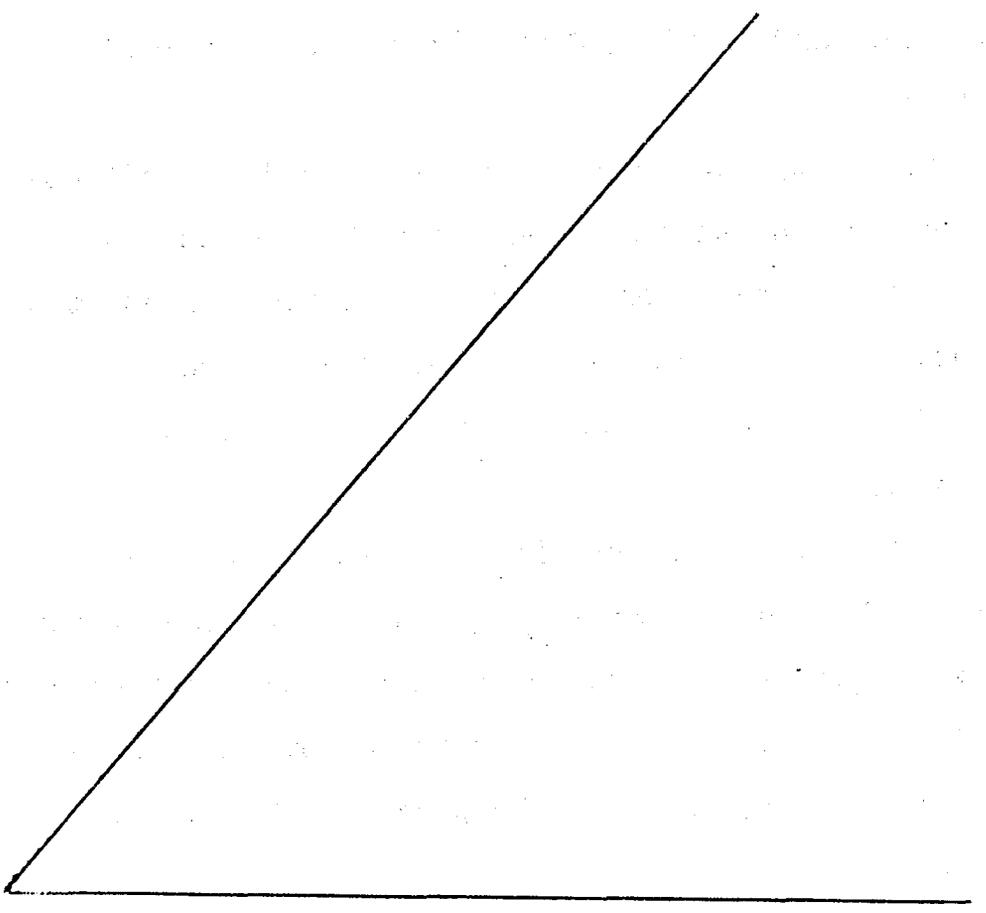
sequences for each random output.

Practical implementation of the invention will now be described, by way of example, with reference to the accompanying drawings in which:

Figure 1 is a circuit diagram of a coding/decoding system hereof;

Figure 2 is a circuit diagram of an imput/display and control system; and

Figures 3 and 4 are flow diagrams.



In the drawings, referring first to Figure 1, a coder/decoder 10 has associated therewith a key code unit 11. The unit 11 serves over lines 12 to control sequences of binary word operation via sequencers 13A, 13B and concerning successive input binary words from lines 14A. Those word operations are shown herein as being sequences representing organisations relative to memories M100 to M115, each organisation comprising a specified number of the memories M100 to M115 and specified effective capacities for those memories M100 to M115.

The number of memories for each organisation in a succession of organisations can be in accordance with a set of random numbers, one per organisation per sequence, say ranging from 8 to 16 for the sixteen memories shown. That set of random numbers is readily stored in the sequencer 13A. In fact, several such sets can be so stored in a read-only memory (ROM) component thereof to be selected by the contents of the key code unit, say one field of a key number. Then, it is only necessary for the write routing circuitry to be subjected to a maximum in sequential energisation of the memories M100 to M115 for each random number and the corresponding organisation

say via a counter in write-routing circuitry WR.

The effective capacities of the memories M100 to M115 in each organisation is also readily prescribed by a set of random numbers ranging from minimum desired to maximum possible word content of each of the memories. In fact, allowing zero to be specified would enable skipping of memories and thus remove the need for restricting write-routing to a maximum and thus the need for storing the first-mentioned set of random numbers. The contents of each of the memories in each organisation correspond to what we have previously called blocks. If desired, there can be a number of such stored sets of memory capacity determining random numbers equal to the number of organisations (n) in a cyclic sequence thereof. Those stored sets may be permutated or at least varied as to start set according to the input key code, say a field of a key code number, to give different choices for different users. Similar or extended effects are achievable by storing more sets (m) and selecting therefrom and/or using a constant from the key code of a modifier for the random numbers.

Control of the memories according to successive random numbers of a set is readily achieved, say via a

counter loaded by such numbers in turn, say each after decrementing the preceding one to zero before moving onto enabling the next memory. It is desired that read out from the memories be in a different order from writing in, and there will normally be different or effectively different sets of random numbers available to the sequencer 13B for controlling the order in which the memories M100 to M115 are read out for each aforesaid organisation of blocks by read out ordering circuitry RO. The latter is readily operative to step from memory to memory by way of pointers recorded therein or in the memories or in the write routing circuitry during storage in the memories.

Binary-to-n permutators, binary-to-n out-of-m coders, and counters operative relative to accumulation are all well known, as are shift registers, ring counters, masking techniques, and selective pointer facilities, so that specific implementation of the sequencers 13A, 13B presents no problems in the art, whether to separate random number stores or to the same store for both of the sequencers 13A, 13B.

It is in fact feasible, and preferred, to avoid any cyclic sequence by using a pseudo-random number generator of a logic circuit type, say the well-known type using shift register means that is long relative to the digit length of the number required and relies upon modulo-2 addition of contents of stages thereof often associated with reentrance of the shift register means.

Then, the key code number will be used as a "seed" for the pseudo-random generator outputs from which will be used to defer active memories, i.e. number of blocks, memory capacities, i.e. block lengths, and order of reading out to define an organisation hereof. At the end of relevant operations associated with such organisation, the last word output of the pseudo-random generator can and/or a partial combination with the original input, say modulo-2, be used as a "seed" for generation of outputs for the next succeeding operation, and there will be no repetitive overall cycle of organisations. However, a similar logic-circuit based pseudo-random generator will, of course, produce exactly the same outputs for the same input at the same time, i.e. if operated effectively synchronously one at the transmitter and the other at the receiver.

Finally, in relation to the memories M100 to M115, we advert to alternative backwards (B) and forwards (F)

operative switches SW and SR so the writing and reading may be in reverse order if desired and or is advantageous in avoiding frequency inversion for enhanced unintelligibility and a relative improvement in that no clue is available as to reversal, certainly not by simple passage through a tape recorder.

As shown, the coder/decoder 10 also supplies coded output data words to lines 14B and suitable timing enable circuitry is included for controlling responses of various items hereof so that coding is performed and outputs taken as required, say with the memories M100 to M115 effectively operating as a coding buffer store. An accurate clock is required and such is indicated at C.

The input data words are supplied by a latch circuit 15 from an analogue-to-digital converter 16 itself supplied with audio signals via a band-pass filter 17, preamplifier 18 and amplifier 19 from a suitable input such as a microphone to terminal 20 or loudspeaker to terminals 21 according to the state of switch or relay 22.

Thus, input analogue signals (audio) are prepared for amplitude sampling by the analogue-to-digital converter 16, which is conveniently free-running and with appropriate discrimination, say 256 levels for audio. The latch 15 will, of course, be sampled at instants

appropriate to operation of the coder/decoder 10. A sampling line 28 is shown for that purpose and includes disable/interrupt logic 26 for ensuring that the latch cannot change while it is being sampled and that, otherwise, each change of the analogue-to-digital converter results in a change of the latch. Sampling of the latch is caused by the signal level on branch line 27 and updating thereof by line 28, change of state of the analog-to-digital converter 16 being signalled on line 29.

Coded data signals from lines 13 are shown applied to a digital-to-analog converter 35 and thence via preamplifier/mixer 36, filter 37 and amplifier 38 to a communications channel 39. The channel 39 may be of a radio type, say the popular CB band radio system, or telephone type, say via an acoustic coupler.

For transceiver operation, i.e. transmission and reception as required in most communication applications, a link 40 is shown between the channel 39 and the junction between relay 22 and band-pass filter 17. In practice, separate switched terminals of the same switch or relay 22, or one ganged therewith, will normally be used.

It should be clear how the above described circuitry will serve for transforming both of input signals and

received signals. However, it is necessary, for communication purposes, that those operations are synchronised to the extent that the successive coding sequences are repeated in step at decoding.

A suitable start synchronisation system could include a plase-locked loop, operative in conjunction with tone generator 46 and start code specifying system 47, though we find that such is avoidable. The main aspect of synchronisation is to ensure that the sequencers at each end are running in step. Basic communication is achieved using a start burst of a prescribed frequency signal from the tone generator 46 at one end. That burst signal is shown injected at 48 after the band-pass filter 17 to mutualise the transmission side, say topped off for that purpose after the amplifier 19 if a phase-locked loop is used. A connection 51 is also shown from the tone generator to the premaplifier and mixer circuit 36 for transmission purposes and resetting of the receiving side.

Operation of a synchronisation switch 52 will operate the tone generator 46 and cause transmission of a burst of synchronisation frequency whereby the receiving unit is brought into basic synchronism. Entry of the same start code at the receiving unit will place

the coder/decoder and sequencer units at the same position in their sequences of codes for the same transmitted signal. That will largely do away with further plase-locked loop type synchronisation especially if any slight log is within an overcapacity of the memory system M100 to M115, and there is a preferably unique delay representing a number of nominal cycle times of the coder/decoder 10. Then, the sending of said synchronising signal from the transmitting station to the receiving station starts the coder/decoder delay times at the transmitter and receiver, effectively taking account of whatever is the transmission time over channel 39. Appropriate specification of any desired start code is via the system 47, which may include delay determining means or simply pass the start code to the coder/decoder for calculation of the delay required. The system 47 is shown connected via an interfacer 53 to the coder/decoder 10 for setting purposes. In a programmed microprocessor system, the interfacer 53 would simply be to a data bus branched to lines 13 and communications between the microprocessor, its data memory and its program store.

Usually, the start code specifying system will

include data-entry means, in the form of key switches or touch-sensitive pads, and display means, usually digital. Details of a system suitable for that and other purposes are shown in Figure 2.

In Figure 2, a display 60 has any convenient number of digits of which seven are indicated by input lines 61 via resistors 62. The lines 62 are shown extending to appropriate ones of input key switches 64. There are eight input key switches 64 which are connected in common over resistor 65 to ground potential and are also connected to junctions 66 with eight lines 67 extending between a tristate interfacer circuit 68 and, via resistors 69, a positive voltage line 70 shown including the synchronisation switch 52. The tristate interfacer 68 is operative to take binary signals from and supply them to lines 71 branched from a data bus 72.

The preferred manner of operation is in a normal display mode for data on lines 71 via the interfacer 68. In order to enter data, the line 73 is energised to change from normal display mode to write mode, whereupon all of the junctions 66 go to logic-one except for those connected to key switches 14 that are operated, which go to logic-zero level. There will be automatic display at 60 of what

has been entered.

The key switches 64, when sequentially operated, load digit display segments automatically, such segments being sequentially energised over lines 74. Key entry debounce circuitry is conveniently avoided by employing a program control to effect plural readings of the lines 61 before settling the display, say after ten reads indicate the same result.

The purpose of the synchronisation switch 52 is to ensure that transmissions through the interfacer of entered data takes place after the operator is satisfied with such entry. At that time, of course, for the system of Figure 1, the burst of tone generator output will also be triggered. Also, the contents of each digit position of the display 60 will correspond to a key code word/number.

A microprocessor based system is even more secure as to synchronisation, as such can be left to program control so long as accurate clocks are used. Suitable overall programming is indicated by way of flow charts in Figures 3 and 4 specific implementation of which relative to any particular microprocessor system will be readily apparent to and achievable by those skilled in programming.

Reverting to Figure 2, we also show a programmed

It will be appreciated from the flow charts that the coding system is of a type virtually wholly analogue to the aforementioned pseudo-random number type of operation for Figure 1. Here, however, the effect is relative to one effectively continuous random access memory space (RAM) that is split up into varying numbers and lengths of block spaces effectively nose-to-tail and preferably always filling the available or designated total memory space conveniently called a sheet. Moreover, the sheet will be loaded in "random" specific blocks in a "random" designated order at which read-out word-by-word immediately preceding.

In relation to writing and reading, operation is relative to the same "random" settings for pairs of organisations though the grouping is actually decided in a complementary manner, see address incrementing (block "B Forwards") and decrementing (block "B Backwards"). The latter includes the boxes of the forward block with the indicated variation of the left most box.

The degree of security, i.e. difficulty of unauthorised decoding, is extremely high, especially in circumstances where the input key code number is used to start or "seed" the random number generation for the first pair of organisations and the last produced random number is used, preferably on a random basis of combination or not with the original key word, but for the next pair of organisations and so on. Alternate

forwards and backwards operations are preferred.

Reverting to Figure 2, we also show a programmed microprocessor system comprising a microprocessor chip 80 and data memory 81 interconnected by the data bus 72. A program memory is also shown at 82 connected to an address bus 83 with connections to the data memory 81, the microprocessor chip 80 and to a chip addressing circuit 84 having outputs 85 each for energising a particular chip of the system when such is required to operate according to the program.

In order to utilise such a system for any analogue signals, there is also shown connection to the data bus 72 of analogue-to-digital and digital-to-analogue converters referenced 16 and 35 as for Figure 1. The data bus 72 is also shown connected to the program store 82 in generally conventional manner for a microprocessor system. In general, a read/write control, see line 86, is required for the micro-processor, data store and the digital-to-analogue converter.

For the transmission system of Figure 1, the program memory 82 will contain the desired procedures for data coding and decoding to be effected by the microprocessor chip 80 using data from the data memory 81. Outputs 85 from the chip address circuit 84 will serve to enable such chip(s) as are required at any one time, and thereby readily separate the various

transmission, reception, display and synchronisation functions required.

A particular desirable further feature is indicated at 87 which is a delay circuit operative whenever display is specifically required, which may actually be set from the microprocessor itself, see the two connections thereto, or separately. The purpose of the delay circuit is to assist in multiplexing for the display so that the latter is energised appropriately for display purposes.

It will be evident that circuitry such as the key switch/display/interfacer of Figure 2 is capable of much wider application, as indeed is the further combination with the microprocessor/data memory/program members/chip address elements of the same Figure. However, the system of Figure 2 is found to be particularly effective in the context of the coding/decoding communication system of Figure 1.

Reverting to Figure 1, attention is also drawn to a relay drive circuit 90 that further includes a delay circuit 91 which allows the coder/decoder to complete any actions necessary regarding the current message.

It will be appreciated that the system of Figure 1

can be inherently selective as to operation with and without coding/decoding. Thus, if entry to the coder/decoder 10 is via a branch from a bus that is continuous through 114A and 114B, input signals can traverse the circuitry through the analog-to-digital and digital-to-analog converters without necessarily being operated upon by the coder/decoder. Accordingly communications contact can be established between two similarly equipped stations in a normal uncoded manner, and the coding/decoding activated by use of the synchronisation system at any later time. Moreover, operation without the analog-to-digital and digital-to-analog converters, i.e. entirely digitally, would give excellent security for direct data communications say between computer installations and over public channels.

CLAIMS

1. A method of scrambled communications signalling wherein signals as transmitted and received are in a coded form representing a reorganisation of original information signals made with reference to binary words representing successive original information components by reorganisation according to sequentially different organisations which organisations comprise variable lengths (numbers of binary words) and numbers of blocks of said binary words in variable sequences different from original information order so that said signals are time-different from said original signals.

2. A method according to claim 1, wherein binary word reorganisation is preceded by analogue-to-digital conversion and succeeded by digital to analogue conversion for communications using analogue coded signals from analogue original signals.

3. Transmitter apparatus for the method of claim 1 or claim 2 comprising a plurality of binary word stores for binary word outputs representing original information and corresponding to said blocks, means for defining effective word capacities

of said stores and thus particularise block lengths for each said organisation and means for selectively defining a block order at least relative to reading binary words from said stores which order will correspond to a said organisation.

4. Receiver apparatus for the method of claim 1 or claim 2, comprising a plurality of binary word stores for binary words representing coded received signals, means for defining effective binary word capacities of said stores and thus particularise block lengths corresponding to block organisations at transmission coding, and means for selectively defining an order for reading binary words from said stores and thus particularise block orders in each block organisation at transmission coding.

5. Apparatus according to claim 3 or claim 4, comprising code input means for selectively setting a particular coded cyclic sequence of organisations.

6. Apparatus according to claim 5, comprising display means for showing and thus checking coded input.

7. Apparatus according to any one of claims 3 to 6, with provision for storing and reading operations relative to said stores to be in opposite directions for the same store.

8. Transceiver apparatus comprising apparatus

according to any one of claims 3 to 7 with means for determining transmission and receiving codes of operation.

9. Apparatus according to any one of claims 3 to 8, wherein said stores comprise snappings on a random needs memory associated with a microprocessor programmed for required storing and reading operations.

10. Apparatus according to any one of claims 3 to 9, comprising tristate interfacing means for key-controlled data input lines also connected to display means.

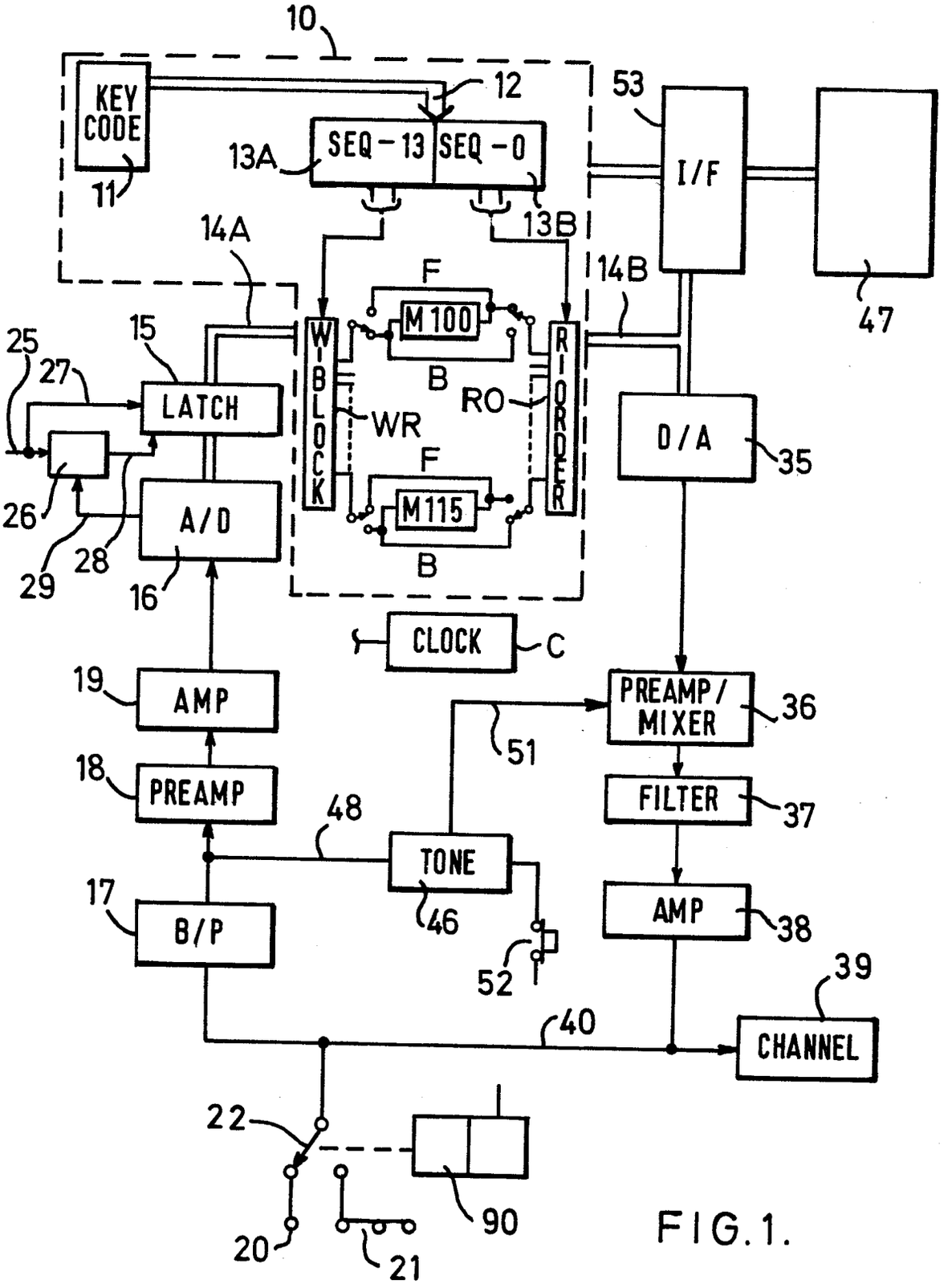

10
KEY CODE
11
12
SEQ - 13
SEQ - 0
13A
13B
53
I/F
47
14A
14B
F
M 100
B
RO
WR
F
M 115
B
W BLOCK
R ORDER
25
27
15
LATCH
26
29
28
A/D
16
D/A
35
CLOCK
C
19
AMP
18
PREAMP
17
B/P
48
TONE
46
51
52
PREAMP/ MIXER
36
FILTER
37
AMP
38
39
CHANNEL
40
22
20
21
90

FIG. 1.

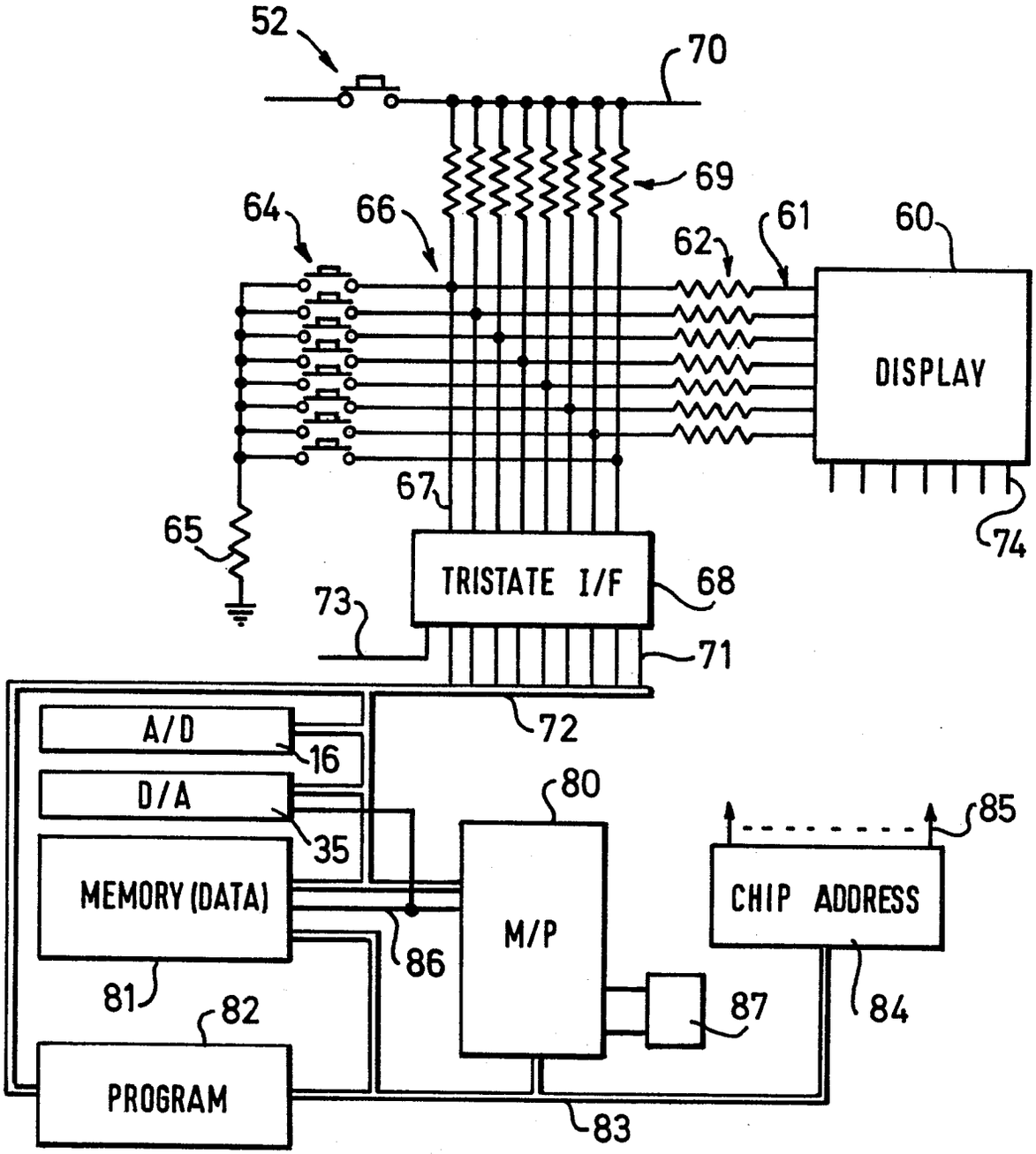

52
70
69
64
66
61
60
62
DISPLAY
67
65
74
TRISTATE I/F
68
73
71
72
A/D
16
D/A
35
80
85
MEMORY (DATA)
M/P
CHIP ADDRESS
86
87
84
81
82
PROGRAM
83

FIG. 2.

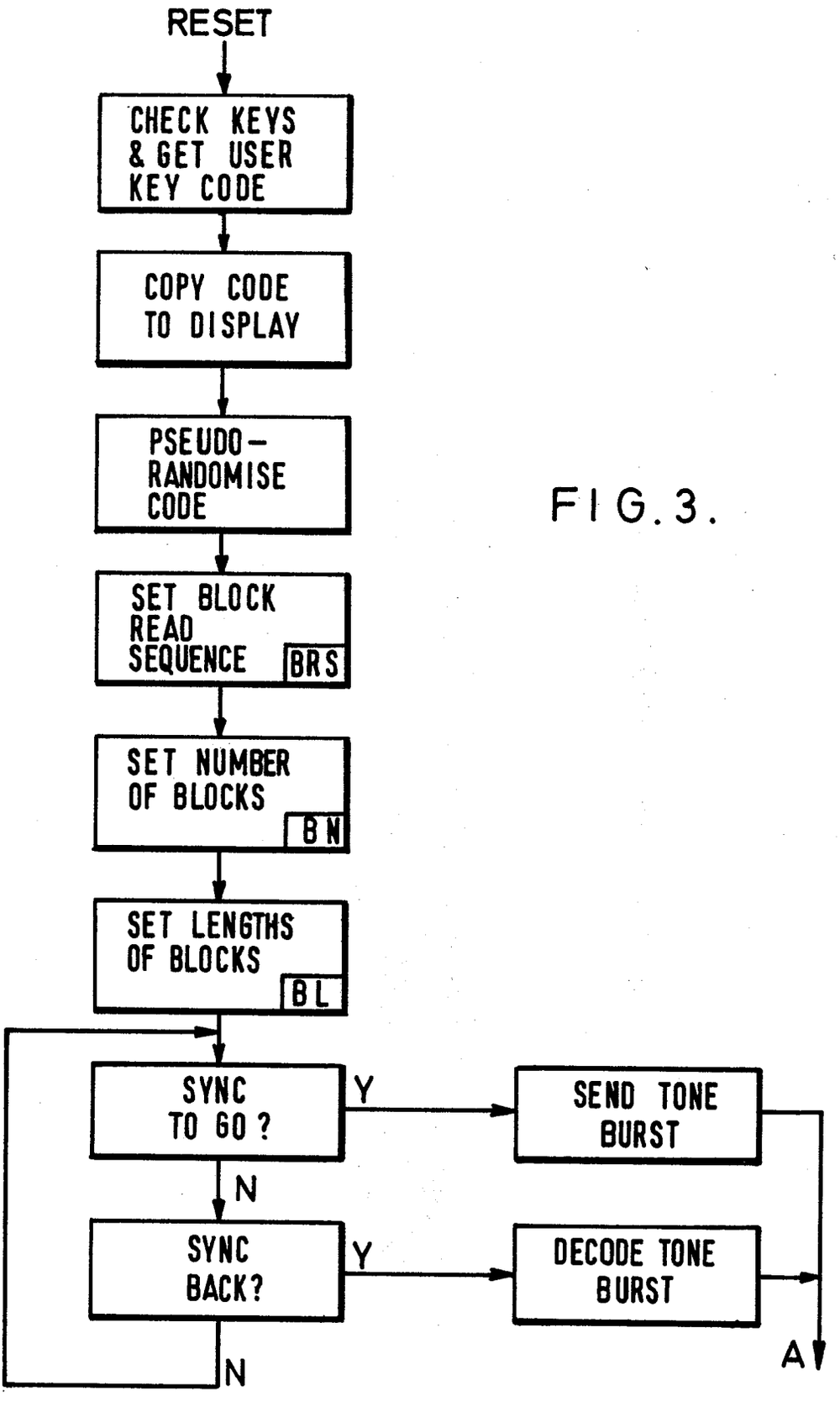

RESET
CHECK KEYS & GET USER KEY CODE
COPY CODE TO DISPLAY
PSEUDO-RANDOMISE CODE
SET BLOCK READ SEQUENCE
BRS
SET NUMBER OF BLOCKS
BN
SET LENGTHS OF BLOCKS
BL
SYNC TO GO ?
Y
SEND TONE BURST
N
SYNC BACK?
Y
DECODE TONE BURST
N
A

FIG.3.

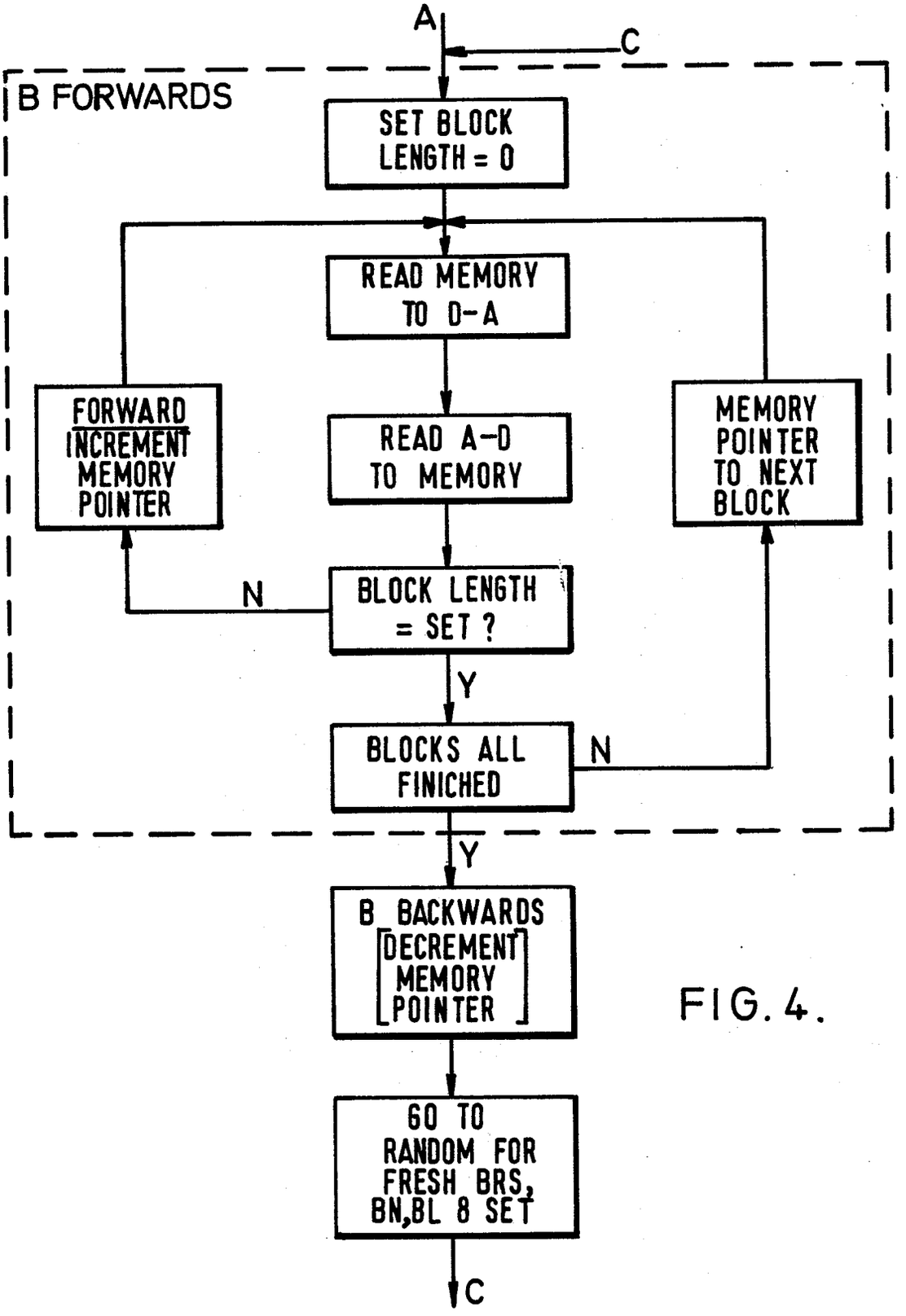

A
C
B FORWARDS
SET BLOCK LENGTH = 0
READ MEMORY TO D-A
FORWARD INCREMENT MEMORY POINTER
READ A-D TO MEMORY
MEMORY POINTER TO NEXT BLOCK
N
BLOCK LENGTH = SET ?
Y
BLOCKS ALL FINICHED
N
Y
B BACKWARDS [DECREMENT] MEMORY [POINTER]
GO TO RANDOM FOR FRESH BRS, BN,BL & SET
C

FIG. 4.