United States Patent

Jackson

[15] **3,701,019**

[45] **Oct. 24, 1972**

[54] **ALARM SYSTEM USING CODED SIGNALLING**

[72] Inventor: **Charles L. Jackson**, Arlington, Mass.

[73] Assignee: **Signatron, Inc.,** Lexington, Mass.

[22] Filed: **March 25, 1970**

[21] Appl. No.: **22,503**

[52] **U.S. Cl.** **325/64,** 325/55, 325/364

[51] **Int. Cl.** **H04b 1/04,** H04b 1/16

[58] **Field of Search**........325/31, 32, 40, 55, 64, 364, 325/122; 179/1.5, 15 BA; 178/22; 340/146.1, 258, 348

[56] **References Cited**

UNITED STATES PATENTS

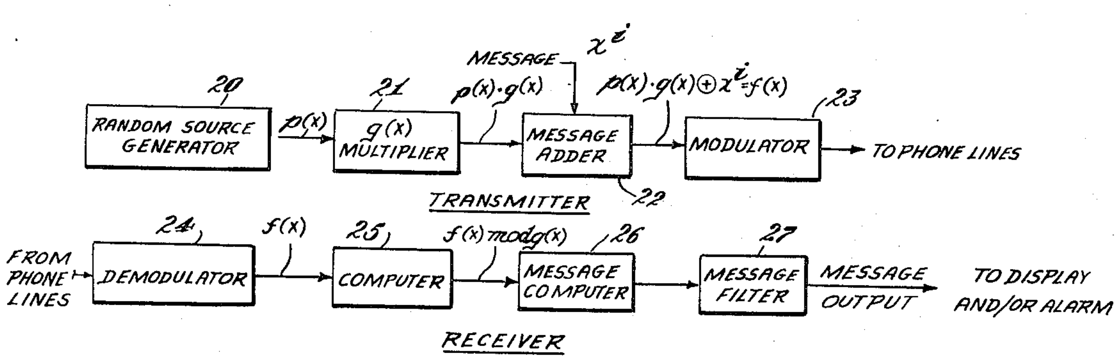
3,466,601	9/1969	Tong	340/146.1
3,380,023	4/1968	Magnuski	340/147
R23,601	12/1952	Hamming	177/353
3,278,903	10/1966	Long	178/22 X
2,701,305	2/1955	Hopper	250/27

Primary Examiner—Robert L. Griffin
Assistant Examiner—Kenneth W. Weinstein
Attorney—Roberts, Cushman & Grover

[57] **ABSTRACT**

A signaling system for detecting at a central station a message from a remote location at which one or more different messages can be generated. A coded signal is generated at the remote location and an "error" uniquely determined by the message to be transmitted is inserted into the coded signal and the altered signal transmitted. A receiver at the central station is arranged to detect the presence of such inserted "error" so as to correctly identify the message that has been transmitted, whereby such message can be displayed or used to activate an alarm device.

10 Claims, 4 Drawing Figures



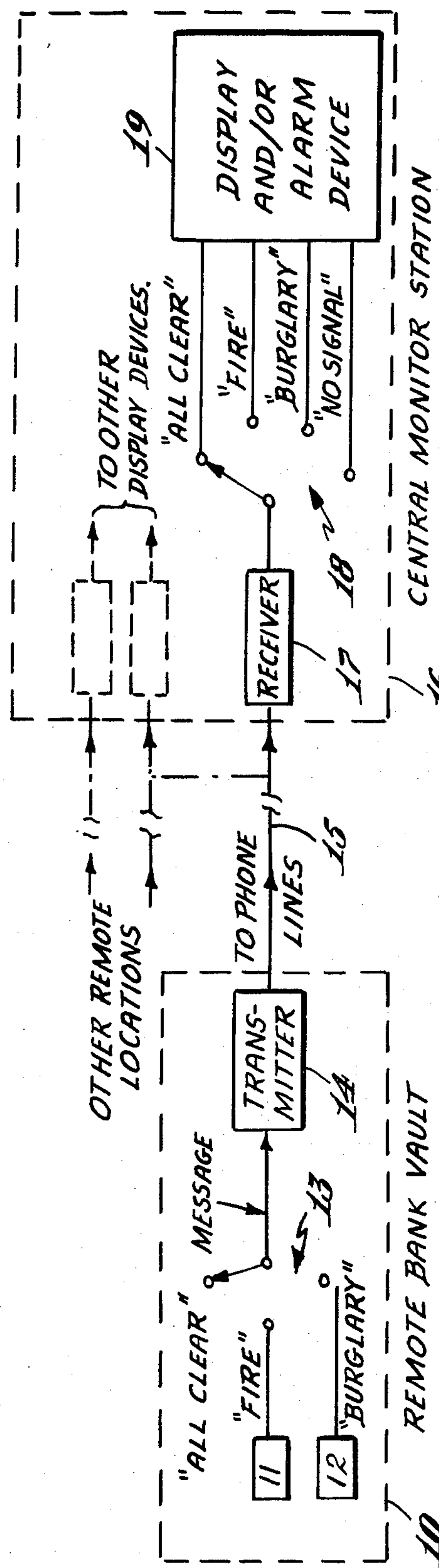

OTHER REMOTE LOCATIONS
TO OTHER DISPLAY DEVICES.
"ALL CLEAR"
"FIRE"
"BURGLARY"
"NO SIGNAL"
DISPLAY AND/OR ALARM DEVICE
19
RECEIVER
17
18
16
CENTRAL MONITOR STATION
TO PHONE LINES
15
TRANS-MITTER
14
MESSAGE
13
"ALL CLEAR"
"FIRE"
"BURGLARY"
11
12
REMOTE BANK VAULT
10

Fig. 1

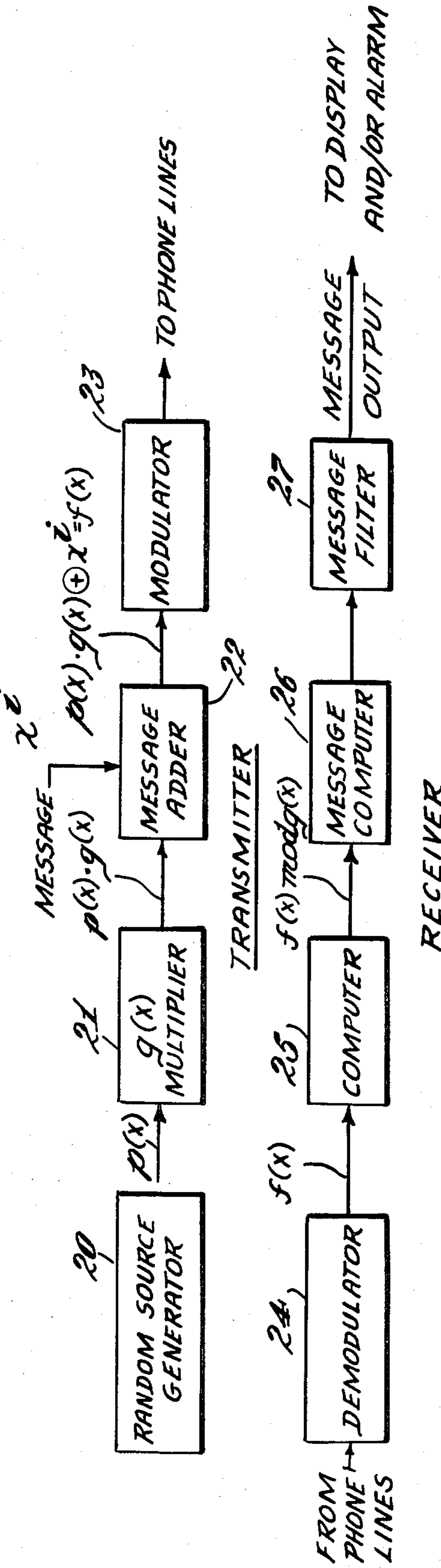

RANDOM SOURCE GENERATOR
20
p(x)
g(x) MULTIPLIER
21
p(x)·g(x)
MESSAGE
x^i
MESSAGE ADDER
22
p(x)·g(x)⊕x^i=f(x)
MODULATOR
23
TO PHONE LINES
TRANSMITTER
FROM PHONE LINES
DEMODULATOR
24
f(x)
COMPUTER
25
f(x) mod g(x)
MESSAGE COMPUTER
26
MESSAGE FILTER
27
MESSAGE OUTPUT
TO DISPLAY AND/OR ALARM
RECEIVER

Fig. 2

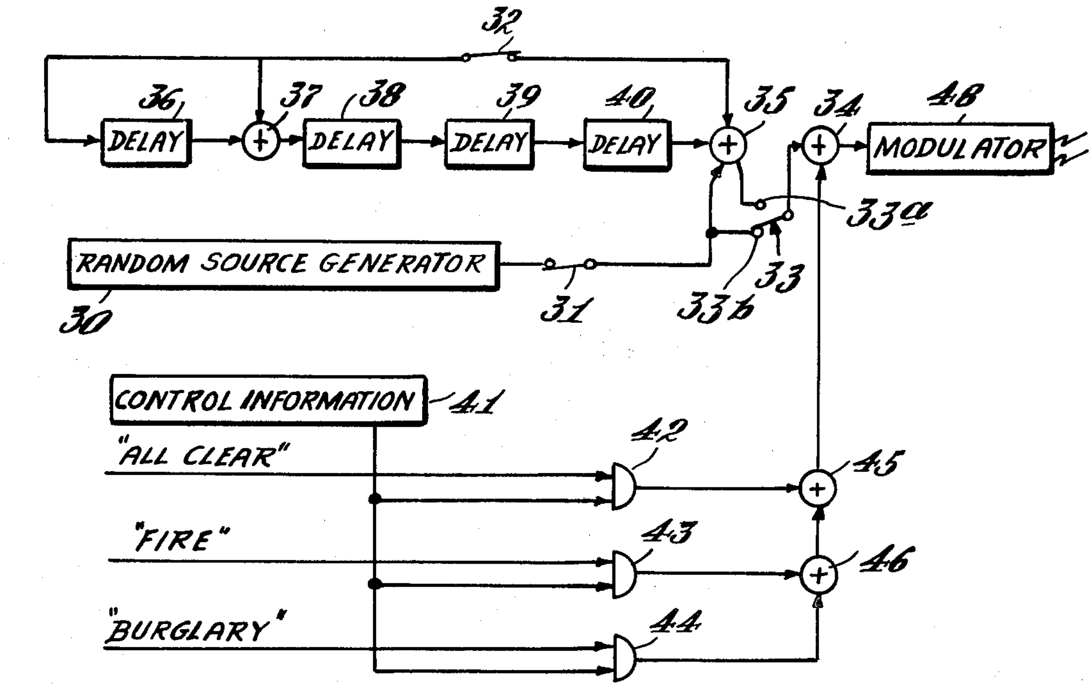

32
36
37
38
39
40
35
34
48
DELAY
DELAY
DELAY
DELAY
MODULATOR
33a
RANDOM SOURCE GENERATOR
33
30
31
33b
CONTROL INFORMATION
41
42
"ALL CLEAR"
45
43
"FIRE"
46
"BURGLARY"
44

Fig. 3

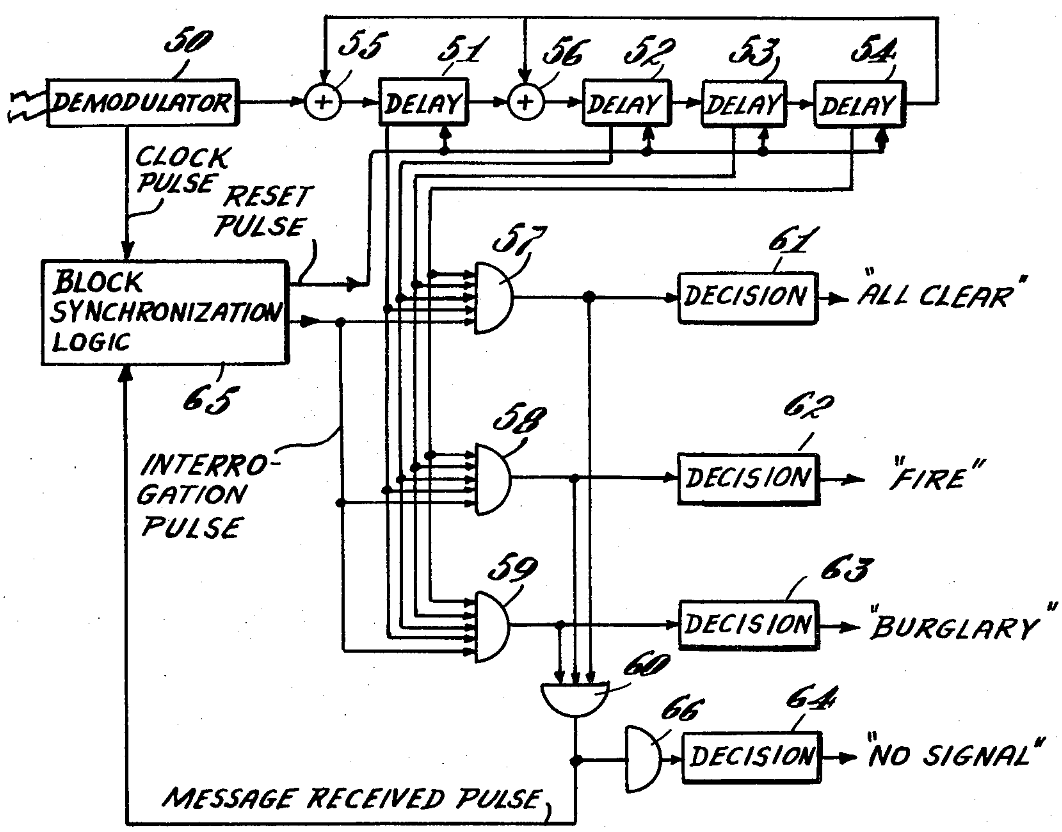

50
55
51
56
52
53
54
DEMODULATOR
DELAY
DELAY
DELAY
DELAY
CLOCK PULSE
RESET PULSE
57
61
BLOCK SYNCHRONIZATION LOGIC
DECISION
"ALL CLEAR"
65
58
62
INTERRO-GATION PULSE
DECISION
"FIRE"
59
63
DECISION
"BURGLARY"
60
66
64
DECISION
"NO SIGNAL"
MESSAGE RECEIVED PULSE

Fig. 4

ALARM SYSTEM USING CODED SIGNALLING

This invention relates generally to signaling systems and, more particularly, to such systems which are adapted for use as remote signaling alarm apparatus, particularly those in which the alarm signals can be communicated over voice or teletype grade land lines.

In remote alarm signaling systems which are utilized to provide fire alarm, burglary alarm, or all clear signals from a remote location or from one or more such remote locations to a central monitoring station, for example, it is desirable that the signaling system provide adequate communication security and also utilize techniques for assuring suitable message verification at the central station as well as a reduction of false alarm signals which may be extraneously generated, such as by noise on the lines. In such systems it is desirable that the alarm signal be "scrambled," that is, placed into a coded form, and transmitted to the central location where it can be appropriately "de-scrambled" or decoded and the desired message signal or signals identified from the coded format. In addition, the system should not require excessively elaborate equipment, particularly in commercial applications, since it is desirable to keep the costs of manufacture and maintenance of the system as low as possible, while at the same time making it sufficiently difficult for an intruder either to bypass the system or to otherwise render it ineffective, such as by inserting false messages into the system.

In presently available remote alarm systems it is often relatively easy for an intruder to monitor the transmission line so as to intercept and determine the message content thereof, or to determine a change in the message content thereof, or even to insert a false message into the system. Thus, a sophisticated intruder, for example, may find it possible to insert an "all-clear" signal even though his own activity would normally have generated a burglary alarm signal to indicate that an intrusion has taken place. Thus, if the system can be so tampered with, his actions are effectively masked from the central monitoring station.

This invention is designed to make it extremely difficult, if not substantially impossible, for the above tampering activities to be accomplished effectively, even should an intruder find it possible to monitor the transmission line in some manner. Moreover, the invention is arranged to provide an appropriate indication if a continuing loss of a message signal occurs so that faults in the system can be readily detected. At the same time the system of the invention is further designed to allow some momentary or transient loss of the transmitted signal, without indicating a loss of the message, so that communications are improved by reducing the false alarm rate of the system during operation.

The above aspects of the invention are accomplished by a unique method of coding the transmitted message which coding process when operated in conjunction with a complementary decoding process at a receiver station produces an effective system for accomplishing the above purposes at a relatively low cost of manufacture and maintenance.

The coding system of the invention is based upon the properties of cyclic codes and, more specifically, utilizes a random signal generator which produces a first block of information comprising a series of random information bits. By appropriate means the random bits are utilized to generate a second block of information comprising a series of redundant information bits bearing a unique relationship to the random information bits from which they are derived. Prior to the transmission of an assembled signal comprising such random and such redundant information bit blocks, one of a plurality of suitably produced message signals is selected to provide a change in the value of one of the information bits in the assembled signal, thus, producing an assembled signal having an effective "error" at a specified bit position in the assembled signal, which error with reference to the remaining unchanged information bits has a unique relationship to the message signal it is desired to transmit.

The assembled signal which has been so altered is thereupon appropriately transmitted and ultimately received at a centrally located monitoring station. At such station a complementary "error decoding" system is utilized so as to identify the position of the changed information bit. Identification of the position of the changed information bit appropriately identifies the correct message signal which has been transmitted and a suitable audible or visual display or alarm can be generated at the monitor station.

Because the altered assembled signal which is so transmitted effectively contains a randomly arranged set of information bits, an intruder, without a knowledge of the code being used, is unable to identify the location of the altered bit and, thus, is unable to identify the message content thereof or to substitute a different message without detection at the monitor station. Without such capability, the intruder is unable to know the security status of the remote location which is being protected and is likewise incapable of inserting a false message for transmittal to the receiving station. Such a system, as described more specifically below, is adaptable to the use of relatively inexpensive components for its implementation and, therefore, its cost of manufacture, installation, and maintenance is relatively low.

The invention is described in more detail with the help of the accompanying drawings wherein:

FIG. 1 shows a block diagram of an overall environment in which the system of the invention can be used;

FIG. 2 shows a simplified block diagram of the transmitter and receiver portions of the system shown in FIG. 1 which operates in accordance with the general principles of operation of the invention;

FIG. 3 shows a more detailed block diagram of one embodiment of a transmitting unit of the invention; and

FIG. 4 shows a more detailed block diagram of one embodiment of a corresponding receiving unit of the invention.

In FIG. 1 the overall system block diagram shows an environment in which the status of a remote location, such as a bank vault **10**, is to be monitored by a central monitoring station **16** so that its condition, for example, with respect to the presence of fire or the presence of an intruder, such as a burglar, may be appropriately determined.

For this purpose suitable sensing elements **11** and **12** of known configuration, not described in further detail here, may be used to detect fire or burglary activity and thereby produce suitable message signals (denoted as the "Fire" and "Burglary" signals in the figure) at their output terminals. An appropriate message selector shown schematically as switch **13** thereby picks up either one of such message signals or, alternatively, an "All Clear" signal, such picked up signal then being fed to an encoding transmitter **14**. The transmitter, described in more detail below with reference to FIGS. **2** and **3**, then transmits a coded signal containing such message signal to appropriate land lines, such as telephone lines **15**, which signal is received at the central monitoring station **16** by a suitable receiver unit **17**, the structure and operation of which is described in more detail with reference to FIGS. **2** and **4**. Receiver **17** decodes the incoming message to determine the status of the remote location and in turn provides an indication of such status, through an appropriate message selector, shown schematically as switch **18**, by suitably displaying whichever message signal was generated at the remote location or by actuating an alarm, as shown by the display and/or alarm device **19**. As explained in more detail below, any continuing loss of such transmitted signal during the transmitting and receiving process will be indicated by the "No Signal" condition situation but only if such loss extends over a preselected time period. In this way a momentary loss of signal, due to some line fault or other transient problem, will fail to signify a "No Signal" condition and false alarms of that nature will be avoided. Other similar channels may be established, as shown, with respect to additional remote locations.

Basically the concept of using an appropriate cyclic code can be explained briefly as follows. It is known that a correspondence can be established between binary vectors and polynominals with binary coefficients by mapping the vector components onto the coefficients of the polynominal. For example, if a binary vector has the values (1, 1, 1, 0), this binary vector can be mapped onto the polynominal:

$$1+1\cdot X+1\cdot X^2+0\cdot X^3 \qquad (1)$$

which expression reduces to a polynominal of the form:

$$1+X+X^2 \qquad (2)$$

Multiplication and addition of polynominals can be defined as, for example, if a polynominal $p(X)=X$, and a polynominal $g(X)=1+X$, then

$$p(X)\cdot g(X)=X+X^2, \text{ and} \qquad (3)$$

$$p(X)\oplus g(X)=1 \qquad (4)$$

where the symbol "$\oplus$" is used to represent "addition mod 2" which is in effect an "exclusive-OR" operation, while the symbol "$\cdot$" is used as the familiar multiplication symbol.

FIG. **2** shows a simplified block diagram of transmitted unit **14** in which a random source generator **20** generates a sequence of random information bits, or digits, such generators being readily available and well known to those in the art. As discussed more fully below, the random source generator generates a sequence of bits the total number of which can be selected in accordance with an appropriate code as discussed more specifically below.

Random source generator **20** is used to produce a series of random bits which can be mapped into a representative polynominal $p(x)$ which can then be multiplied by an operating polynominal $g(x)$ to form a polynominal $p(x)\cdot g(x)$, as represented by block **21**, which thereupon represents the assembled signal prior to any alteration by a message signal. The message signal, represented by the designation x^i, is then added to the assembled signal, as represented by block **22**, to produce an altered assembled signal $f(x)$ which is equal to the previously assembled signal plus the message signal, as represented by the polynominal:

$$f(x)=p(x)\cdot g(x)\oplus x^i \qquad (5)$$

where the symbols are defined above. Such signal is appropriately modulated by a conventional modulator **23** and fed to the transmission lines. At the receiver unit the incoming signal is appropriately demodulated by a conventional and corresponding demodulator **24** and the resulting signal $f(x)$ is fed to an appropriate computer component **25** to produce the signal $f(x)$ mod $g(x)$. Given such signal it is relatively easy to compute the correct message signal via a message computer **26** which message signal is appropriately fed through a message filter **27**, the operation of which is discussed more fully below, to produce the message output which can be thereupon utilized at the display and/or alarm device.

In the above operations the message signal x^i can be thought of as an inserted "error" in the signal $p(x)\cdot g(x)$ and the computers **25** and **26** at the receiver are set up to detect such inserted "error" which appropriately identifies the message being sent. Each message input signal at the transmitter end produces a unique identification signal at the receiver end and, thus, if false messages are inserted they will not produce any of the expected identification signals at the receiver and a "No Signal" condition will be designated to indicate that something is at fault in the system. Such fault, for example, may include a break in the line which prevents the transmission of any signal at all or the transmission of a false signal inserted by an intruder. In any case such "No Signal" indication represents a condition which must be investigated by the system operator.

FIG. **3** shows a more detailed block diagram of a transmitter unit which effectively implements the desired operations for permitting the transmission of an altered assembled signal, while FIG. **4** shows a more detailed block diagram of a corresponding receiver unit for effectively decoding the incoming transmitted signal which has been so altered and thereupon to identify the message signal which has been transmitted.

In FIG. **3** a random source generator **30** generates a series of random information bits, the number of which can be selected in accordance with an appropriate code. For example, if the total transmitted signal is comprised of a periodic coded signal of 15 bits, or digits, the random source generator may be utilized to generate the first eleven bits, each of which in a simple binary system has a randomly selected value of either "0" or "1". During such time, switches **31**, **32** and **33** are in the positions shown in FIG. **3**, that is, switches **31** and **32** are closed while switch **33** has its center arm connected to terminal **33b**. Such bits are fed to a first "exclusive-OR" gate **34** and to a second "exclusive-OR" gate **35**. The output of gate **35** is fed to the input of a first conventional flip-flop delay, or shift register, circuit **36**, having a time delay equal to the time between successive bits, the output of which is fed, together with the input thereof, to a third "exclusive-OR" gate **37**. The output of gate **37** is fed to a series of similar flip-flop delay circuits **38**, **39**, and **40** and, thence, to the second input terminal of "exclusive-OR" gate **35**. Following the generation of the first eleven random information bits from random source generator **30**, switches **31**, **32** and **33** are placed in the alternate positions that is, switches **31** and **32** are opened and switch **33** has its center arm connected to terminal **33***a*.

Thereafter, four additional bits of the total fifteen bit transmission block are generated as a result of the operation of circuits **36**, **38**, **39** and **40**, the values of such additional bits thereby being uniquely determined by the values of the first eleven randomly generated bits. The four additional bits are referred to as "redundant" information bits.

The eleven random information bits and the four redundant information bits generated therefrom, thus, are effectively assembled and effectively represent the coefficients of a polynominal signal $p(x)\cdot g(x)$ at the input of "exclusive-OR" gate **34**, the second input of which is fed with an appropriate message signal as described below. In the exemplary embodiment under discussion there are shown, for example, three messages which can be transmitted to the centrally located monitor station, such message sources being identified therein as "All Clear," "Fire" and "Burglary." The active message sources, in this case the "Fire" and "Burglary" message sources, are received from appropriate sensors which produce such messages in the form of appropriate output signals only if the corresponding conditions exist. The "All Clear" signal is provided so as to be produced at gate **34** only if no fire or burglary signals are present, the use of such signals all being controlled in accordance with a control information unit **41**.

For example, each such message unit sources is connected to an input of one of a plurality of parallel AND gates **42**, **43**, and **44**, respectively, the other inputs of which are each fed with the signal from control information unit **41**. Since an output appears from an AND gate only when both inputs are present, control information unit may be arranged to produce pulse output signals at arbitrarily selected bit positions in the fifteen bit sequence and applied to the AND gates **42–44** in a uniquely selected manner. For example, if such pulses are selected to occur at bit positions **5**, **8**, and **11**, the pulse at bit **5** being applied only to gate **42**, the pulse at bit **8** being applied only to gate **43**, and the pulse at bit **11** being applied only at gate **44**, an output will occur from gate **42** at bit position **5** only if an "All Clear" signal is simultaneously present, from gate **43** at bit position **8** only if a "Fire" signal is simultaneously present, and from gate **44** at bit position **11** only if a "-Burglary" signal is simultaneously present. The outputs from AND gates **43** and **44** are fed to an appropriate "exclusive-OR" gate **46** and the outputs from AND gate **42** and "exclusive-OR" gate **46** are fed to an "exclusive-OR" gate **45**, so that only a single desired message is supplied to the second input of "exclusive-OR" gate **34**.

In the example under consideration, if the "All Clear" signal is supplied from exclusive-OR gate **45** in accordance with the above selected message controlling unit, a change in the value of the fifth bit in the previously assembled 15-bit signal occurs so that the output of exclusive-OR gate **34** represents an altered assembled signal which is changed uniquely in accordance with the "All Clear" message. Such an altered assembled signal is then fed to an appropriate modulator **48** which provides a modulated output signal for transmission by suitable phone lines.

The altered assembled information signal is received at the receiver, shown in more detail in FIG. **4**, where it is first appropriately demodulated by a demodulator **50** in a manner well-known in the art. The receiver has a complementary "error" correction subsystem which comprises a plurality of delay flip-flop, or shift register, circuits **51**, **52**, **53** and **54** in conjunction with "exclusive-OR" gates **55** and **56**, as shown, such configuration being effectively complementary to the corresponding elements in FIG. 3. The outputs from flip-flop delay circuits **51–54** are fed to a plurality of decoder elements **57**, **58** and **59**, each of which is arranged to provide an output signal only when all of its input signals have uniquely related values.

Synchronization of the received signal with the transmitted signal is provided through a block synchronization logic unit **65** which is actuated by a clock pulse which is appropriately derived in a well-known manner by the demodulator from the transmitted signal received from the remote location. The synchronization logic unit supplies a reset pulse so as to place each of the shift registers into their initially desired states (wherein their outputs are zero) at the beginning of each decoding computation cycle. It also supplies an interrogation pulse to each of the decoder elements **57–59** so as to produce the desired message signal indication after the incoming received signal has been operated upon by the delay circuits **51–54** as described in more detail below. When the delay circuit operation is complete the outputs from the delay circuits are uniquely determined by the particular message signal which was inserted into the altered assembled signal as transmitted. In accordance with the values of the output signals from circuits **51–54**, a signal will then appear at the output of only one of the decoder elements **57–59**, provided one of the desired message signals has been so inserted at the transmitter. If no message signal was inserted in the transmitted assembled signal or if the transmitted signal is lost in transmission, the probability of obtaining an output from any of the decoder elements **57–59** is substantially reduced.

If an output is obtained from any of the decoder elements **57–59** (showing that a message signal was received), an indication that such an output is present is provided at the output of "OR" gate **60** and a "-Message Received Pulse" therefrom is appropriately fed back to block synchronization logic unit **65** so that such unit can supply a reset pulse signal to the delay circuits to place them in readiness for decoding the next incoming transmitted signal. An inverter element **66** is connected to the output of gate **60** and is arranged to produce an output only when no input signal thereto is present so that, if no message signal has been received, a "No Signal" condition will be indicated by the display or alarm device.

Each of the outputs of elements **57–59** and that of inverter element **66** is fed through an appropriate decision making circuit **61**, **62**, **63**, and **64**, respectively. Each such decision making circuit may be in the form of a filter circuit, e.g., an R-C network followed by a discriminator circuit, or in the form of a suitable digital counting circuit. In either case, the circuit is arranged to permit an appropriate message signal to be supplied to the display and/or alarm device for indicating visually or audibly the status of the remote location only if an input signal continues to be applied to such circuit over an arbitrarily selected time period determined by the circuit characteristics. Thus, during such a selected time period several blocks of 15-bit input signals, each block containing the same message information, will have been received and operated upon by the decoding circuits. By the use of such decision making circuits, false alarms can be considerably reduced.

In coding an appropriate sequence of random and redundant information bits, both a polynominal $g(x)$, identified as the generator polynominal, and a number "k," identified as the number of random information bits in a block, can be selected. Such choices, once having been made, remain fixed and thereby define the code which is to be used. Thereupon, a block consisting of "k" random information bits is generated, such block representing a corresponding polynominal $p(x)$. Having selected the polynominal $g(x)$, the quantity $p(x)\cdot g(x)$ is effectively computed by the shift register circuits which provides a bit sequence corresponding to the coefficients of such computed polynominal. Such bit sequence includes the random information bits plus the redundant information bits, the number of the latter being determined by the order of the selected polynominal $g(x)$. To the polynominal $p(x)\cdot g(x)$ a polynominal M_i, with only its i^{th} coefficient non-zero (i.e., with only an x^{ith} component) is added, which operation produces an altered polynominal $f(x)=p(x)\cdot g(x+M_i)$, the coefficients of which represents the altered bit sequence signal which is thereupon transmitted. At the receiving end the polynominal $p(x)\cdot g(x)$ is effectively subtracted from the polynominal $p(x)\cdot g(x)+M_i$ to provide M_i. By varying the position of the non-zero i^{th} coefficient in the polynominal M_i, different messages can be transmitted and subsequently identified, as discussed with reference to the specific examples described below.

The transmitter-receiver system of FIGS. **3** and **4** effectively implements such operation, although with a slight modification in order to make such implementation somewhat simpler. For example, rather than computing the polynominal $p(x)\cdot g(x)$ in order ultimately to produce $f(x)$, the configuration shown therein effectively computes $f(x)$ such that

$$f(x)=s(x)\cdot g(x), \text{ and} \tag{6}$$

$$f(x)=p(x)\cdot X^m+r(x), \tag{7}$$

where m equals the number of redundant information bits (i.e., the order of $g(x)$, the generator polynominal) and a remainder polynominal $r(x)$ has an order less than m. Such alternate computation method has substantially the same effect, as far as the system operation is concerned, as that generally discussed with reference to FIG. **2** although its implementation as described in FIGS. **3** and **4** is somewhat simpler. As an example, the following selections may be made:

$$m=4$$

$$g(x)=x^4+x+1, \text{ and}$$

$$k=11$$

Thus, rather than computing the quantity $p(x)\cdot g(x)$, in FIG. **3** it is simpler to compute the quantity $f(x)$ such that

$$f(x)=p(x)\cdot x^4+r(x),$$

where the degree of $r(x)$ is less than 4 and $r(x)$ has been selected to make $f(x)$ divisible by $g(x)$.

There are a large number of possible different combinations of m, $g(x)$ and k available for use in selecting the coding desired. One subclass of such coding is given by the so-called "Hamming Codes" which codes, for example, are described and discussed in E. R. Berlekamp, "Algebraic Coding Theory," McGraw-Hill Book Co., 1968, Chapter 5 and W. W. Peterson, "Error Correcting Codes," The M.I.T. Press-John Wiley & Sons, Inc., 1961, Chapter 8. Such codes are characterized in that, when the degree of polynominal $g(x)$ is m, (equivalent to the total number of redundant information bits), "k" is equal to 2^m-1-m. Thus, for a degree of $g(x)$ equal to **4** (i.e., $m=4$), k is equal to 11 and the use of 4 redundant digits provides a total block length of 15 bits. The shift register configurations described in FIGS. **3** and **4** correspond to the selection of such a 15-bit Hamming code having four redundant information digits.

Accordingly, other Hamming codes could be used. For example, if m is equal to 5, k is equal to 26 and the total block length is 31 bits utilizing 26 random information bits and 5 redundant information bits. If m is equal to 3, k is equal to 4 and the total block length is 7 bits, with 4 random bits and 3 redundant bits. The more bits used, the more complex the signals and, hence, the more difficult it is for an intruder effectively to break the code which is used in his efforts to tamper with the system's operation.

As a specific example, let it be assumed for simplicity that a 7-bit Hamming code is selected for use and, accordingly, that the random generating source produces a sequence of 4 random information bits and 3 redundant information bits, the generator polynominal being selected as x^2+x+1. More specifically, for example, if the sequence of generated random bit values are 1101, such sequence corresponds to the coefficients of a polynominal:

$$p(x)=x^3+x+1 \tag{8}$$

In such a system the configuration of the shift registers used to implement the code is substantially the same as shown in FIGS. **3** and **4** except that registers **40** and **54** are omitted. If the random bit sequence is fed to such a delay circuit configuration and the shift registers all have initial values of zero, a three redundant bit sequence 000 is produced. Such sequence, when combined with the four random information bits provides an assembled signal having the bit sequence 0001101, which represents the coefficients of a polynominal of the form:

$$p(x) \cdot x^2 + r(x) = x^6 + x^4 + x^3, \text{ where} \quad (9)$$

$$r(x) = 0 \quad (10)$$

If an "All Clear" message is to be sent and such message signal is arbitrarily selected to alter the value of the fifth bit position in the sequence (i.e., the coefficient of x^2 in the above polynominal), an altered bit sequence of the form 0011101 is obtained for transmission, such signal having an effective "error" at such position.

At the receiver end the incoming altered signal is appropriately demodulated and fed to the delay circuit configuration, which configuration effectively operates to divide the input signal $f(x)$ by the generator signal $g(x)$ so as to produce the remainder signal $r(x)$ the coefficients of which appear as the outputs of each of the delay circuits when the division operation is completed. The remainder signal is uniquely determined by the change that has been inserted by the message signal at the transmitter unit. Thus, for example, in decoding the incoming signal to indicate the presence of the "All Clear" message inserted at the transmitter, the output signals at each of the delay circuits following their operation on the incoming assembled signal produces a sequence of output bit values of 100 in the example under discussion. It is clear that a different, but unique, sequence of output values at the delay circuits will be obtained in the presence of message signals from the "Fire" and from the "Burglary" channels.

The decoding elements **57–59** then are arranged to provide outputs only if their inputs from the delay circuits have the unique values associated with each message signal. Thus, for the "All Clear" signal discussed above, decoder element **57**, for example, would be provided with three inputs **100** from delay circuits **51**, **52** and **53** (circuit **54** is omitted for the 7-bit Hamming code under discussion) and one interrogation pulse input. Element **57** is, thus, arranged to produce an output only if its inputs have the unique relationship 1001 (i.e., the outputs from shift registers **57–59** plus the presence of an interrogation pulse).

Thus, the decoding system at the receiver has effectively detected the "error" in the incoming circuit and has provided an indication of what that "error" uniquely represents in terms of the message signal transmitted by the transmitter at the remote location. Similar procedures can be utilized using the same general principles for the more complex case where a 15-bit Hamming code signal is used (using the exact configurations shown in FIGS. **3** and **4**), or a higher number of Hamming code bits, or where cyclic codes other than Hamming codes are used.

In accordance with the invention, then, effective security against eavesdropping and tampering is provided. No matter what message is sent, the transmitted bit stream effectively appears as a random bit stream to an intruder and it is substantially impossible to detect the message content. Thus, if the system is being used as a burglary alarm system device, for example, an intruder cannot monitor the line with unsophisticated detection equipment, such as a voltmeter or an oscilloscope, to determine when and if an alarm has gone off or if the alarm system has even begun its signaling process.

What is claimed is:

1. A signaling system comprising
   - means for generating an initial sequence of random information bits:
   - encoding means including means responsive to said generating means for generating a sequence of redundant information bits derived from and bearing a unique relation to said initial sequence of random information bits;
   - said encoding means further including means for producing a cyclicly encoded assembled signal comprising said sequences of random and redundant information bits;
   - means for producing a message signal;
   - means for changing the characteristics of said first encoded assembled signal at a specified bit position thereof in response to said message signal to produce an altered assembled signal having an effective error determined by the changed characteristics at said specified bit position;
   - means for transmitting said altered assembled error signal;
   - means for receiving said altered assembled error signal;
   - error detection means including: decoding means having a configuration for providing operation complementary to said encoding means and being responsive to said received altered assembled signal so as to produce a signal uniquely determined by said effective error in said altered assembled signal; and
   - means responsive to said uniquely determined signal for producing an output signal which indicates said specified bit position to identify said message signal.

2. A signaling system in accordance with claim 1 wherein said message signal generating means includes a plurality of message sources; and
   - means for selecting the output from one of said message sources to produce said message signal.

3. A signaling system in accordance with claim 1 wherein said receiving means is at a central monitoring station and said transmitting means is at a location remote therefrom, and said signaling system further includes
   - means at said central station for displaying said identified message signal.

4. A signaling system in accordance with claim 1 wherein said first assembled signal is assembled in accordance with an error correcting code and said characteristic changing means changes the value of said assembled signal so that said detection means produces a unique message signal.

5. A signaling system in accordance with claim 1 wherein said first assembled signal is assembled in accordance with an error correcting code and said characteristic changing means changes the value of said assembled signal at a single bit position therein.

6. A signaling system in accordance with claim 4
   - wherein said first assembled signal comprises a fifteen bit Hamming code signal including eleven random information bits and four redundant information bits and
   - wherein said message signal generating means includes
     - means for generating a plurality of message signals;

means for selecting one of said message signals so that the value of said first assembled signal is changed at a different bit position depending upon which message signal is selected for transmission.

7. A signaling system in accordance with claim 1 wherein

said random information bit generating means produces a sequence of random information bits corresponding to the coefficients of an operating polynominal p(x);

said redundant information bit generating means includes

a plurality of shift register means and exclusive-OR gate means arranged in a configuration corresponding to a generator polynominal $g(x)$, whereby said first assembled signal comprises a sequence of random and redundant information bits corresponding to the coefficients of an output signal $p(x) \cdot g(x)$; and

said characteristic changing means adds to said first assembled signal a message signal corresponding to a polynominal x^i to produce an altered assembled signal $f(x)$ in response to said message signal; and

said detection means includes

a plurality of shift register means and exclusive-OR gate means arranged to provide a plurality of information bits corresponding to the coefficients of a remainder polynominal $r(x)$ representing the remainder resulting from a division of the received altered assembled signal $f(x)$ by the generator polynominal $g(x)$;

said remainder polynominal being uniquely determined in accordance with said message signal.

8. A signaling system in accordance with claim 1 wherein

said transmitting means includes means for modulating said altered assembled signal to provide a modulated transmitted signal; and

said receiving means includes

means for demodulating said received modulated signal for producing a demodulated altered assembled signal; and

means for synchronizing the operation of said detection means with the reception of said received altered assembled signal.

9. A signaling system in accordance with claim 1 and further including means for providing a signal at said receiving means indicating the absence of a message signal in said transmitted signal.

10. A signaling system in accordance with claim 9 wherein said determining means further includes a plurality of decision making circuits for producing an indication of the presence or absence of a message signal only when said message signal, or the absence of any said message signal, has been determined for a selected time period.

* * * * *