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

(11) Publication number: **0 216 595**
A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 86307139.5

(51) Int. Cl.⁴: **H 04 K 1/06**

(22) Date of filing: 16.09.86

(30) Priority: 17.09.85 GB 8522979

(43) Date of publication of application:
01.04.87 Bulletin 87/14

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

(71) Applicant: **GEC AVIONICS LIMITED**
Airport Works
Rochester Kent ME1 2XX(GB)

(72) Inventor: **Brierley, William Edward**
28 Crown Way
Southminster Essex(GB)

(74) Representative: **Hoste, Colin Francis et al,**
The General Electric Company p.l.c. Central Patent Department (Chelmsford Office) Marconi Research Centre West Hanningfield Road
Great Baddow Chelmsford CM2 8HN, Essex(GB)

(54) Data encryption.

(57) Data transmitted over any sort of "broadcast" system can, in general, be picked up by anyone with the correct sort of receiver properly tuned in. For many reasons, however, it may be desirable for the data signals to be "scrambled" or encrypted, before transmission so that only the recipient who can appropriately "unscramble" or decrypt the signal, will be able to see the data in its original plain form.

The invention provides a data encryption/decryption method (and the equipment therefor), in which plain form data is transferred sequentially through two sets of analogue shift registers at a number of different transfer rates such that for each register data fed in at one rate is then fed out at another; whereby the data transferred between the two sets of registers is encrypted, but when fed out of the last register is decrypted, and in plain form.

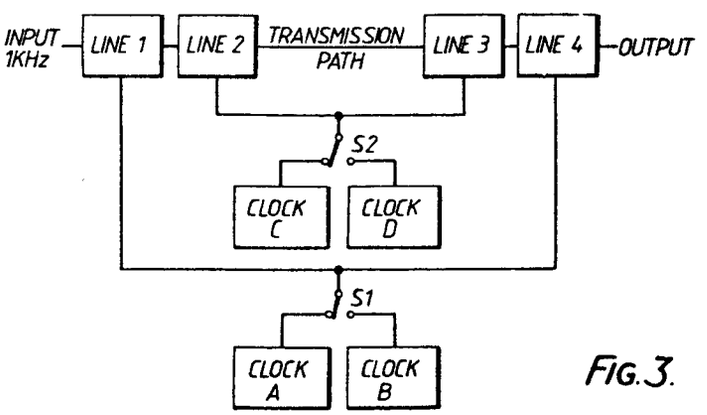

FIG. 3.

EP 0 216 595 A2

0216595

DATA ENCRYPTION

This invention concerns data encryption, and relates in particular to the encryption of analogue data, such as speech, for transmission over a narrow band channel, and to the received signal's subsequent de-cryption to reconstitute the data in its original form.

Signals transmitted over any sort of "broadcast" system, best exemplified by radio, can in general be picked up by anyone with the correct sort of receiver properly tuned in. For many reasons, however, it may be desirable for the signals to be intelligeable only to the intended, and thus authorised, recipient, and to ensure this it is common to "scramble", or encrypt, the data before transmission, so that only the recipient who can approprately "unscramble", or decrypt, the signal will be able to see the data in its original plain form.

Such a data tranception system is said to be a "secure" system, in that the data involved is secure against eavesdroppers. As might be expected, however, there are different levels of security - some encryption methods are so simple (and cheap) they can be recognised, and the appropriate de-cryption technique worked out and applied within a few minutes, while others are so complex (and expensive) they may take hours, days or even years to crack. Naturally, the type of encryption employed is chosen to fit the security level required.

In one known method of data encryption there are two

sequential registers and two different transfer rates, and for each register data that has been clocked in (filling up the register) at one rate is clocked out at the other. Thus, for each register the data clocked out represents a frequency-shifted version of the data that was clocked in. It is this frequency shifting that encrypts - and subsequently decrypts - the data. For each register the shifting may be up or down and that in fact it will alternate from one to the other. The reason for this alternation is simple: data clocked in at a first rate is clocked out at a second, but as it is so clocked out naturally a further batch of data is being clocked in, at this second rate, to be clocked out in its turn at the first rate, and so on. Accordingly, a batch of data clocked in at the lower rate and out at the higher rate is up-shifted, while the next batch, necessarily clocked in at the higher and out at the lower rate, is down-shifted (and the next batch is up-shifted, the next down, and so on).

The invention relates to the encryption, and subsequent decryption, of data, specifically narrowband analogue data typified by speech (the human voice contains almost all its output in the band fron 300 Hz to 3000Hz); purely for convenience, hereinafter the invention is described mainly in terms of its application to the encryption/decryption of speech.

Typical users desirous of having their speech

communications rendered unintelligible to unintended and unauthorised recipients are the Police, who prefer criminals not to be able to gain useful information by listening in to police radio broadcasts, the Military, who are against the Enemy making use of overhead battlefield (and other) conversations, and Businessmen, who do not wish their commercial rivals to be able to make sense out of any telephone conversations to which they may become a party. For a Police car radio network, where the information transmitted is usually for immediate action, only a low level of security is required, but for a Business discussion of long term plans a much higher level is desirable.

Many different data encryption systems have been proposed; all have advantages and disadvantages. The present invention suggests a novel system that is at heart extremely simple (and thus cheap) but can be elaborated to almost any degree of complexity. It can, therefore, be of value whether the situation requires a low or a high level of security.

In one aspect, therefore, the invention provides a data encryption/decryption method, in which: first and second registers are associated with encryption and a third and fourth with decryption, plain-form data is transferred sequentially through the four analogue shift registers such that data element is clocked at different clocking rates and for each register data which is fed in

at one clocking rate is then fed out at another; and data is fed into a third register at the same clocking rate as it was fed out of the second register, and is fed out of the third register at the same clocking rate as it was fed into the second register; and data is fed into the fourth register at the same clocking rate as it was out of the first register and is fed out of the fourth register at the same clocking rate as it was fed into the first register, whereby, by virtue of the resulting frequency shifting, the data transferred between the second and third registers is encrypted, but when fed out of the fourth register is decrypted, and in plain form.

In another aspect the invention provides a data encryption/decryption method in which a first register is associated with encryption and a second and a third register are associated with decryption; plain form data is fed into the first register at a series of clock rates and then fed out of the first register at a different series of clock rates and fed into the second register at the same series of clock rates it was fed out of the first register at, when the second register is full the data being fed out of the first register is fed into the third register at the same series of clock rates it was clocked out of the first register at and the data in the second register is fed out at the same series of clock rates it was fed into the first register at, when the third register is full the data being fed out of the first

register is fed into the second register at the same series of clock rates it was fed out of the first register at and the data in the third register is fed out at the same series of clock rates it was fed into the first register at, and this cycle of use of the second and third registers is repeated; the series of clock rates supplied to the registers being such that; data transferred between the first register and the second and third registers is encrypted, and the data output of the second and third registers is plain form and the the duration of time taken to fill or empty each of the registers with data is a constant.

In a further aspect the invention provides analogue data encryption/decryption equipment which includes: four shift registers arranged in a sequence; tranception means whereby the output of the second register can be supplied to the input of the third register, input means for feeding plain-form data to the first register; output means for feeding plain-form data from the fourth register; clock pulse means for each register, for giving a sequence of different clock signals to the registers to control the transfer of their contents therethrough; and synchronisation means enabling the clock pulse means for each register to be synchronised one with the other, such that, when plain form data is transferred sequentially through the four registers at four different clocking rates (a) for each register, data which is fed in at one

clocking rate is then fed out at another, and (b) data is fed into the third register at the same clocking rate as it was fed put of the second register, and is fed out of the third register at the same clocking rate as it was fed into the second register, (c) data is fed into the fourth register at the same clocking rate as it was fed out of the first register, and is fed out of the fourth register at the same clocking rate as it was fed into the first register.

In another aspect the invention provides data encryption/decryption equipment which includes: a first shift register associated with encryption and a second and a third shift register associated with decryption; tranception means whereby the output of the first register can be supplied to the inputs of the second or third registers; input means for feeding plain form data to the first register; output means for feeding plain form data from the fourth register; clock pulse means for each register for giving a sequence of different clock signals to the registers to control the transfer of their contents therethrough; synchronisation means enabling the clock pulse means for each register to be synchronised one with another; and switching means enabling sections of the output of the first register to be supplied alternately to the inputs of the second and third registers, each section being one register full of data, arranged such that, when plain form data is transferred through the register at

a plurality of different clocking rates, for each register data which is fed in at one clocking rate is fed out at another, data is fed into the second register at the same rate it was fed out of the first, data is fed out of the second register at the same rate it was fed into the first, data is fed into the third register at the same rate it was fed into the first and data is fed out of the third register at the same rate it was fed out of the first.

The invention relates to the encryption, and subsequent decryption, of data. As mentioned hereinbefore, this data could be of any type, but the invention is primarily concerned with analogue speech signals - that is, voice signals that occupy the relatively narrow (~3KHz wide) band from about 300Hz to about 3000Hz. Specifically, the invention is intended for use in a voice communications system wherein speech data is encrypted at one location, transferred to another location, and there decrypted. The communications system may be of any sort; two examples are telephone (wired) networks and radio (wireless) networks. In the former there are at the two locations the telephones that are connected to each other possibly by an Exchange of some sort, while in the latter there are at the two locations the transmitter and the receiver, the one launching into the "aether" information-carrying electromagnetic radiation to be received by the other.

The data to be transferred by the inventive method - the input data - is described as plain-form data, to distinguish it from the encrypted data actually transferred between the two locations. It may, in fact, be "plain-form", and not encoded in any way except that necessary for its actual transferral through the system (as, say, voice sound is converted into electrical pulses, and then electromagnetic pulses, and back again to sound, for transception in any radio system), and indeed it is thought to be the main use of the inventive method that uncoded voice sound can be simply and cheaply scrambled into intelligeable form, and then unscrambled. It is not impossible, however, that the input data could already be encoded/encrypted, in which case "plain-form" has merely the aforementioned distinguishing meaning.

In one method of the invention the data is transferred sequentially through four analogue shift registers - it is input to one, transferred ("clocked") through that one and out, and then it is input to a second, transferred through this other and out. The encrypted date is then transmitted to a second location where it is input to a third shift register, clocked through it, then input to a fourth register, transferred through it and out. The data is input to the first register in plain form, is output from the second register - and input to the third register - in encrypted form (as will be explained below, the encrypted form is merely a

frequency-shifted version of the plain form), and is output by the fourth register in plain form. In any system using the inventive method to secure data being transferred between locations, the first and second registers are at the transmitting location, the third and fourth registers are at the receiving location, and the data transferred between the two locations is encrypted.

This aspect of the invention requires at least four analogue shift registers (though in more complex forms, it may use more - six say, pre-encrypting the data and then post decrypting it with an additional fifth and sixth registers.) An analogue shift register is an electronic device having a sequence of elements, or cells, in each of which may be stored an electrical charge the value of which may be any within some continuous range. This sequence of cells is a register, and because the contents can represent - be analogous to - any value (within some range) it is an analogue register. The contents of each cell may be shifted - clocked - to the sequentially next cell under the control of transfer clock pulses suitably delivered to the device (so the register is a shift register), and by doing this an electrical signal/value presented to the first cell may be transferred into that cell, then shifted to the next cell, ... and finally transferred to, and out of, the last cell. The process is very like pouring water from one bucket to the next in a chain of buckets (indeed, one form of such a device is

actually known as a "bucket brigade device"); water - the signal - is poured into the first bucket, and thence to the next, and the next....and so on till it reaches, and is poured out of, the last bucket. It will be obvious that any signal fed into the cell sequence is delayed - over a signal bypassing the sequence - by the time it takes to transfer it through and out of the cells. Clearly, this transfer time is a function of the clock frequency. The lower the frequency - the lower the rate of clock pulses driving the transfer from one cell to the next - the longer it all takes.

If an analogue signal is presented to - and input to - an analogue shift register, and if, as it is input, so it is transferred on and through the register at a rate at or greater than the minimum required by the Nyquist rule (sampling rates must be at least twice the frequency of the input signal's highest frequency component), then the output signal will consist of a series of pulses, or bits, that faithfully define - and in effect are - the original input signal together with a clock frequency component added thereto. By filtering off this clock component there may be reconstituted the original input signal, albeit in delayed form.

Most analogue shift registers are those electronic devices known as Charge Coupled Devices (CCDs). They may contain any number of cells - usually 2^n, where n is from 5 to 10 (i.e, from 32 to 1024 cells) - though 512 cell

CCDs are common. They may also be clocked at any rate (though the time taken to transfer charge from one cell to the next is finite, and thus limits the clocking rate), but typical rates are 1 to 100KHz.

When using analogue shift registers it is normal to clock signals through them at a constant rate. However, in some applications - conversions between different television frame systems, for example - it is the practice to clock the signal in at one rate (until the register is full), and then out at a different rate. This has the effect of comprising or stretching the signal. A compressed signal - the same number of pulses, or bits, but in a shorter time - has a higher frequency than the original input form; it is a frequency-upshifted version of the original signal. Conversely, a stretched signal - the same number of bits, but in a longer time - has a lower frequency than the original input; it is a frequency-downshifted version of the original. In either case the frequency is shifted by a factor of the ratio of the input to the output clock rates. Thus, if a signal at frequency F_{in} is clocked in at rate R_{in} and clocked out at rate R_{out} then the frequency F_{out} of the output signal is given by

$$F_{out} = \frac{F_n . R_{out}}{R_{in}}$$

As an example, if a 3KHz sinewave input signal (F_{in}=3KHz) is clocked in at 10KHz (R_{in}=10KHz) and out at 20KHz

(R_{out}=20KHz) then the output signal frequency F_{out} is $3.\frac{20}{10}$ = 6KHz. Conversely, if the 3KHz signal was clocked in at 20KHz and out at 10KHz then the output signal frequency is $3.\frac{10}{20}$ = 1.5KHz.

In the basic method of the invention there are four sequential registers, and four different transfer rates, and for each register data that has been clocked in (filling up the register) at one rate is clocked out at another. From the foregoing explanation, it will therefore be appreciated that for each register the data clocked out represents a frequency-shifted version of the data that was clocked in. It is this frequency shifting that encrypts - and subsequently decrypts - the data; it is discussed in more detail hereinafter, but here it should be noted that for each register the shifting may be up or down, and that in fact it will alternate from one to the other. The reason for this alternation is simple: data clocked in at a first rate is clocked out at the second, but as it is so clocked out naturally a further batch of data is being clocked in, at this second rate, to be clocked out in its turn at the first rate, and so on. Accordingly, a batch of data clocked in at the lower rate and out at the higher rate is up-shifted, while the next batch, necessarily clocked in at the higher and out at the lower rate, is down-shifted (and the next batch is up-shifted, the next down, and so on).

For each register the alternation of the two rates

itself occurs at a rate that is a function of the length of the registers (the number of cells) and the two clocking rates, for it occurs as each register is filled up with the data clocked in. Though not all analogue shift registers behave in quite the same way, it is for convenience sufficient to assume that a device clocked at, say, 10KHz is having its cell contents transferred at a rate of 10,000 per second, so that a 1024-cell device would be filled (or emptied) in about a tenth (=1024/10,000) of a second. A similar device clocked at 20KHz would thus be filled (or emptied) in about a twentieth (=1024/20,000) of a second. Using such a device, and 10 and 20 KHz clock rates, alternation would occur at 0.1, 0.05,0.1,0.05.....(and so on) second intervals. The effect on a voice signal is very confusing!

The four clock rates may be different by almost any factor, as low as 1.1 times still provides an acceptable scrambling effect.

It is a feature of the method of the invention that the data that is fed into the third register is so fed in at the same rate as it was fed out of the second register, the data that is fed out of the third register is so fed out at the same rate it was fed in to the second register, the data that is fed into the fourth register is so fed in at the same rate as it was fed out of the first register and the data that is fed out of the fourth register is so

fed out at the same rate as it was fed into the first register. This, coupled with the alternation of the rates for each register, results in the data passing between the two pairs of registers being in encrypted form (either up- or down-shifted) while the data that exits the fourth register is in decrypted, plain form (for its encrypted version has been either down- or up-shifted, as appropriate).

The data passing between the two sets of registers is frequency shifted, and thus encrypted. Moreover, the shift alternates between being an up shift and being a down shift and the amount of up or down shifting is not constant. It is perhaps this constant variation in direction and amount of frequency shifting that renders the method of the invention particularly effective, especially with voice data, where the main energy lies at the lower end of the frequency range (300 to 1000Hz, say) but the intelligence - the "formants" - lies mostly at the upper end of the range (2000 to 3000 Hz, say). By shifting the formants back and forth between, say, twice and a half the usual frequencies, and by doing this fairly frequently, so that the ear/brain has no time to adapt, so the voice signal is rendered quite unintelligeable.

As stated hereinbefore data is fed into each register at one rate and out of that register at another rate, data is fed sequentially through the four registers, data is fed out of the fourth register at the same rate at which

it is fed into the first and data is fed out of the third register at the same rate at which it was fed into the second. The rate at which data is fed in/out is determined by clock pulses fed to the relevant register to cause the transferral of its contents, cell-by-cell, into, through and out of the device, and thus is dependent on a clock pulse rate. In order to ensure that these events are in time one with another it is necessary, when putting the invention into operation, to employ some method of synchronising the application to each register of the four different sets of clock pulses. In principle, this merely requires that, sent either alongside or buried within the coded data, there is a master timing signal that enables the fourth register's timing system to synchronise with the first register's system and the third register's timing system to synchronise with the second register's system. For example, commonly each pair of two registers will have its own, nominally independent, clock - the heart of the timing system - that is crystal-controlled to keep very accurate time. This clock signal can then be used to derive the needed different timing signals for each register of the pair. However, even clocks such as these tend to "drift" off frequency as time goes on, so there will be some way of re-triggering the clock cycle from an external source. If, then, each pair of registers' timing system is associated with trigger pulse transmitting/receiving means, such that the encrypting

registers' timing system can send to the decrypting registers' timing system a suitable trigger pulse at some appropriate time, then that pulse can be caused to re-trigger the decrypting registers' clock, and place the two clocks in perfect synchronisation. In one more particular example of synchronisation, discussed further hereinafter with reference to the accompanying Drawings, it is arranged firstly that an unencrypted tone be transmitted from the encrypting to the decrypting register, either continuously (and subsequently filtered out at the receiver) or at the start of transmission (the tone may conveniently be derived by shaping an output from the encrypt clock generating system and modifying to a - possibly - triangular form, or that suitable for the characteristics of the system). For systems with large group delays the tone frequency should be fairly low, typically 200Hz. At the receiving end the encrypted output from the receiving apparatus per se is fed to a tone decoder/phase locked loop. This generates two outputs. The first output is a dc pulse which is produced on lock up, and is fed to the decryption clock generator as a coarse reset. The clock reference generator is crystal controlled, and its output is fed via a gate to the decryption clock generator. A tone generator derived from an output of the clock generator is set to the same as that at the transmitter. This is compared with the second output of the phase locked tone decoded by means of

a phase sensitive rectifier. If the two signals are not in phase, the rectifier output will consist of a series of pulses whose width will be a function of relative phase. The output is shaped and connected to the gate at the input of the clock generator. As a result a pulse or pulses will be "blanked" at the clock generator input. The tone at the receiver will now slip until it is in phase with the incoming signal, when the phase sensitive detection output disappears. Providing the signals remain in phase, no further blanking occurs.

To allow for crystal oscillator drift, a dc signal can be derived from the PSR to adjust the fundamental crystal frequency for ultra fine adjustment.

For more complex systems, the transmitted tone frequency can be varied to indicate "Time of day" at the transmitter.

This method provides a means of synchronisation which does not indicate encryption information.

In its most basic form the invention employs four analogue shift registers in sequence. This can result in acceptable low level security, but for higher levels the resulting encryption is inadequate.

One simple way to raise the security level is slowly to modify the four clock rates according to some pre-agreed code. Alternatively, the clock pulse trains could themselves be modified - by leaving out the occasional pulse, or even inserting an additional pulse - again in a

prearranged manner. Such changes would have the effect of disrupting the operation of any unauthorised "automatic" decryption device not party to the codes, so making more difficult the work of the eavesdropper.

A number of other possibilities exist. For example, if on a four-register system a fixed period for the overall system delay is adopted, for example 80 milliseconds, then each register would have a nominal delay of 20 milliseconds. However, in place of a fixed clock rate for each period a pulse train could be provided pseudorandomly varying at a slow rate. The two constraints are, firstly, that the maximum spacing between pulses should be less than $\frac{1}{3F}$, where F is the upper frequency response required, and secondly, that the number of pulses within the period when all slots are filled must exceed the number of bits (cells) in the register time.

Another way of improving the security of the encrypted data would be to change the clocking rate, that is, change other than the alternation between two rates in the known system. However, such a change in clocking rate will alter the time taken by data to pass through the system. As a result, data will be either overwritten - resulting in loss of data, or blank areas will appear in the signal.

This problem can be overcome by arranging the clock frequencies supplied to the encrypting register so that the time taken to clock in some set amount of data is a

constant. We shall call this time period the frame time. The simplest such amount to choose is one encrypting register full of data. Thus the signal will effectively be processed as a string of sections of signal, each of these sections of signal being of the frame length T. Each section is fed into the encrypting register at a series of different clock rates and then fed out of the register at a different series of clock rates. Each of the series of clock rates being chosen so that in frame time T the total number of clock pulses supplied to the register is equal to the number of cells in the register.

Each of these sections of signal is encrypted by a number of different frequency shifts because it is read into the register at a series of clock rates and then read out of the register at a different series of clock rates (the number of different clock rates, the order of the clock rates and the clock rates may all be altered). Because the time taken for data representing each section of signal to pass through the register is a constant, problems of overwriting and blank areas in the signal are avoided.

For instance, if a 4096 cell line were used to encrypt the signal, a frame time of the signal 58.368 msec could be chosen and one frame length of signal could be fed into the register at four different clock rates as follows:-

	Clock Rate	No. of Bits	Time Taken
1.	50KHz	1024	10.24 msec.
2.	41.66 KHz	1024	12.288 msec.
3.	35.71 KHz	1024	14.336 msec.
4.	23.81 KHz	1024	21.504 msec.
Total:		4096	58.368 msec.

In the next 58.368 msc. the data in the register is fed out as follows:-

	Clock Rate	No. of Bits	Time Taken
1.	41.66 KHz	1024	12.228 msec.
2.	26.32 KHz	1024	19.456 msec.
3.	31.25 KHz	1024	16.384 msec.
4.	50 KHz	1024	10.24 msec.
Total:		4096	58.368 msec.

The signal section is thus encrypted because each 1024 bit section of it is read in and out of the register at different rates, but the time taken to read the signal section in is the same as the time taken to read the signal out. As the section is read out of the register the next signal section is read in and it is later read out at a third sequence of four clock rates.

The signal is decrypted by reading it into a decrypting register at the same sequence of clock rates it was read out of the encrypting register and then reading it out of a decrypting register at the same sequence of clock rates it was read into the encrypting register. Because this requires one signal section to be read out of

decryption at one rate and the next section to be read into decryption simultaneously at another rate, it will, in fact, be necessary to use two registers to decrypt the signal, the two decrypting registers decrypting alternate signal sections.

Such a system is simplest, and provides the highest degree of encryption, when the encrypting and decrypting registers are of equal size. It would however, be possible to use encrypting and decrypting registers of different sizes. If a system with different sized encrypting and decrypting registers were used, the number of clock pulses supplied in the fixed frame time must not be larger than the capacity of the smallest register.

In order to increase the security level of such a system the length of the encrypting and decrypting registers could be altered. This could not be done while a signal was being transmitted, because it would cause loss of data or the introduction of blank sections into the output signal. However, this could be done in the course of a speech message by altering the register's lengths during pauses.

The signal to be encrypted could, of course, be pre-encoded or encrypted for additional security.

Alternatively, the analogue data - a speech signal, say - can be separated into two bands, lower and upper, and fed to two separate sets of registers operating independently. At the receiver high and low pass filters

would separate the two bands before injecting them into two corresponding separate sets of registers. This method also has the advantage that in each pair of frames the instantaneous time and frequency relationship of pitch and formant is completely distorted, and the clock change ratios can be reduced.

Yet another embodiment enables the speech time sequence to be transformed. If two sets of encrypting registers are connected in series and a signal applied for a time which would fill all the registers, the two sets can then be transposed, and transmitted in reverse order. On reception in two sets of decrypting registers, the contents are again transposed before being clocked out. This method can be combined with any other; the number of registers employed determines the amount of transpositon. Obviously, more registers increases the overall delay. However, transposition would also reduce the relative clock change necessary, and the individual frames could be shorter.

Various embodiments of the invention are now described, though only by way of illustration, with reference to the accompanying Drawings, in which:

Figure 1 is a sequence representing an analogue shift register through which a simple signal is transferred;

Figure 2 is a sequence showing a register like that of Figure 1 having a simple signal transferred through it

at different rates;

Figure 3 is a schematic circuit diagram for a simple form of apparatus applying one method of the invention;

Figure 4 shows how data passes through the encryption/decryption system of the invention;

Figure 5 shows a schematic circuit for a synchronising system for use with the invention, and

Figure 6 is a schematic circuit diagram for apparatus applying another method of the invention.

The sequence of Figure 1 represents the transferral of a simple sine wave signal F through a 16-cell analogue shift register (101). At time T_0 all the cells 1-16 are empty; the signal F is presented to the register's input end (the left as viewed) on the input line (102). If the register receives a clock pulse (at time T_1, not shown in the Figure) then a charge representing the value of the signal at that time is placed in the first cell. A second pulse (at time T_2, also not shown) causes the contents of cell 1 to be transferred to cell 2 and cell 1 itself is then filled with a fresh charge representing the new value of the signal presented thereto at that time. The view at time T_4 shows the situation after three such pulses (in a complete series of $\underline{i}$ pulses). By time T_4, the original cell contents have been successively transferred, via cells 2 and 3, to cell 4, and cells 3, 2 and 1 hold, in that order, the charges representing the value of the signal presented to cell 1 at times T_3, T_2 and T_1

respectively.

By time T_{12} the original cell 1 contents have reached cell 12, and by time T_{16} they have reached the final cell (16) at the output end of the register (the right as viewed). At the next clock pulse the contents of cell 16 are transferred out of the register on the output line (103), and at time T_{22} four such transferrals have occurred. At time T_i the number of these transferrals is i-16; the signal on the output line is a series of pulses that is in essence the original sine wave F with the clock frequency (CF: in this case 16 times the input sine wave frequency) superimposed, and a simple filter will remove it and leave the output signal indistinguishable from the input signal.

The same register is shown in Figure 2, with the same simple sinewave input at frequency F_{in}. However, the sequence shows how the output frequency F_{out} varies as the Clock Rate (CR) alternates from CR_1 to CR_2 and back.

Up to time T_{16} clock rate CR_1 has transferred in the signal, filling the register. In order to illustrate the principle, the Figure imagines that CR_1 was exactly right so as to fill the register with one wavelength in the period T_0 to T_{16}. Thus, $CR_1 = 16\ F_{in}$. If the clock rate were to remain at CR_1 the signal would be transferred on and out, and the output signal would have the same frequency as the input signal - i.e, $F_{out} = F_{in}$. However, if for the period from T_{16} up to T_{32} the clock rate is

halved ($CR_2=\frac{1}{2}\ CR_1$) then the register contents are output at half the rate - i.e, at half the frequency. For this period, then, $F_{out}=\frac{1}{2}F_{in}$.

Of course, also during the period T_{16} to T_{32} a fresh "batch" of signal has been input, but this time at CR_2 rather than CR_1. A full register therefore holds two wavelengths ($CR_2=8F_{in}$), and when - in the subsequent period from T_{32} to T_{48} - this is output at clock rate CR_1 the effect is to make the output signal frequency F_{out} twice that of the input signal (i.e, $F_{out}=2F_{in}$).

The general situation is

$$F_{out}=\frac{CR_{out}}{CR_{in}}.F_{in}$$

meaning that the output frequency is related to the input frequency by a factor that is the ratio of the output to input clocking rates.

Figure 3 shows a schematic diagram for a simple form of circuit according to the invention.

In Figure 3 two pairs of registers (delay lines 1,2 and 3,4) are connected by a transmission path. A 1KHz signal is input to line 1, encrypted and fed to line 2. Line 2 then encrypts the encrypted signal for a second time and this "doubly encrypted" signal is transmitted to line 3. The encryption due to line 2 is decrypted by line 3 and the resulting singly encrypted signal fed to line 4 which removes the encryption due to line 1 to reproduce the unencrypted 1 KHz signal. Four clocks (A, B, C and D) control the data transfer through the registers, clocks A

and B are applied alternately to registers 1 and 4 by switch S1 and clocks C and D are applied alternately to registers 2 aznd 3 by switch S2.

In the general case, with a signal of frequency F_{in} input to line 1 and clocked through through at rates CR_1 and CR_2 alternatly applied, and through line 2 at rates CR_3 and CR_4 alternately applied, the situation is as shown in Figure 4, where a signal of frequency Fin is clocked into the first delay line at clock rate CR1. When line 1 is full the signal is clocked out of line 1 at clock rate CR_2 and and into line 2 at clock rate CR_3.

When line 2 is full the signal is clocked out of line 2 and transmitted at clock rate CR_4.

At a distant location this encrypted signal is received and clocked into line 3 at clock rate CR_4. When line 3 is full the signal is clocked out of line 3 at clock rate CR_3 and into line 4 at clock rate CR_2.

Finally, when line 4 is full, the signal is clocked out of line 4 at clock rate CR_1 as a decrypted signal at frequency Fin.

In this case the encrypted transmitted signal, which is vulnerable to interception, is frequency shifted to a frequency $Fin \cdot \frac{CR_2}{CR_1} \cdot \frac{CR_4}{CR_3}$.

Since the lines 1 to 4 are of equal size and clock frequencies CR_1 to CR_4 are all different, this transmitted frequency will vary among the following four frequencies.

a) $Fin \cdot \frac{CR_2}{CR_1} \cdot \frac{CR_4}{CR_3}$

b) $Fin \cdot \frac{CR_1}{CR_2} \cdot \frac{CR_4}{CR_3}$

c) $Fin \cdot \frac{CR_2}{CR_1} \cdot \frac{CR_3}{CR_4}$

d) $Fin \cdot \frac{CR_1}{CR_2} \cdot \frac{CR_3}{CR_4}$

When applied to speech encryption such a simple system might be expected to suffer severe degradation in speech quality due to the bandwidth increase due to the alternate frequency shifting of the encrypted signal. In practice, over a typical link such as a standard telephone for example, the speech quality is quite impressive, providing good speaker recognition.

The encrypted speech is quite unintelligeable, appearing almost similar to band inversion, but with a "garble" effect.

The block diagram of Figure 5 relates to a way of achieving synchronisation of the encrypting and decrypting registers.

A tone is transmitted either continously (and subsequently filtered out at the receiver) or at the start of transmission. The tone is derived by shaping an output from the encrypt clock generating system and modifying to a (possibly) triangular form, or that suitable for the characteristics of the system. The signal is not encrypted. For systems with large group delays the frequency should be fairly low, typically 200Hz.

At the receiver the encrypted output from the receiver is fed to a tone decoder/phase-locked loop. This generates two outputs. The first output is a dc pulse which is produced on lock-up. This is fed to the decryption clock generator as a coarse reset.

The clock reference generator is crystal controlled, its output fed via a gate to the decryption clock generator. A tone generator derived from an output of the clock generator is set to the same frequency as that at the transmitter. This is compared with the second output of the phase-locked tone decoder by means of a phase sensitive rectifier. If the two signals are not in phase, the rectifier output will consist of a series of pulses whose width will be a function of relative phase. The output is shaped and connected to the gate at the input of the clock generator. As a result a pulse or pulses will be "blanked" at the clock generator input. The tone at the receiver will now slip until it is phase with the incoming signal, when the phase sensitive detection output disappears. Providing the signals remain in phase no further blanking occurs.

To allow for crystal oscillator drift, a dc signal can be derived from the PSR to adjust the fundamental crystal frequency for ultra fine adjustment.

In Figure 6 an analogue speech encoder/decoder includes an encrypting system 8 and a decrypting system 9.

An analogue speech signal is applied at 10 and is

clocked into a 4096 cell shift register 11. The shift register 11 is clocked at a series of different clock rates, these clock rates are derived from a 1 MHz reference frequency generated by a frequency source 12 by a variable divider 13. The variable divider 13 is controlled by a code selector 14 which selects a code in response to the signal provided by a pseudo-random code generator 15.

At the start of a signal to be encrypted the pseudo-random code generator 15 produces a number which is supplied to code selector 14. Code selector 14 comprises a large read only memory containing all possible sequences of clock rates that can be used in the encoding shift register 11, and a memory addressing system. When the code selector 14 receives a number from pseudo-random code generator 15 it uses an algorythm to convert this number to a memory address and uses the sequence of clock rates stored at this memory address. The algorythm used to derive this address is programmed into the code selector 14 before communications are started. Thus even someone possessing an identical receiver to the authorised recipient of a message cannot decrypt the message unless he knows the algorythm being used.

The possible series of clock rates are all sequences of four clock rates, each clock rate being used for 1024 clock pulses and having a total period of 58.368 milliseconds.

Code selector 14 then sets the variable divider 13 to feed the first of these clock rates to the register 11. The number of clock pulses sent to the register 11 is counted by a counter 16 and every 1024 pulses the counter 16 sends a signal to the code selector 14 to change the variable divider 13 to the next clock frequency. Every 4096 clock pulses the counter 16 steps the pseudo-random code generator 15 to its next setting. When the code generator 15 is stepped the code selector 14 uses the algorythm to clock up a new sequence of clock rates. This change in clock rate sequences occurs every 4096 clock pulses - in other words once per register full of data, so the data is clocked out of the delay line at different rates to those at which it was clocked in. Thus the data is encrypted by frequency shifting, because four different clock rates are used in each 4096 pulse cycle, the signal will have four different frequency shifts per cycle.

This encrypted signal is then supplied to a transmitter 17 which transmits it.

The transmitted signal is received by a receiver 18 which supplies it to the input of the decryption system 19.

The decryption system 19 includes two shift registers 19A and 19B. Shift registers 19A and 19B are clocked at clock rates derived from a 1MHz reference frequency generated by a frequency source 20 by variable dividers 21A and 21B respectively. The variable dividers

21A and 21B are controlled by a code selector 22 which is in turn controlled by a pseudo-random code generator 23.

Two switches 24 and 30 are arranged so that at any time one of register 19A and 19B is connected to an input of decrypter 9 and the other is connected to an output of decrypter 9.

When an encrypted signal is fed into the decryption system 9 the switch 24 applies it to the input end of shift register 19A. To decrypt this signal it is read into the shift register 19A at the same sequence of clock rates as it was read out of the shift register 11.

This is achieved by the pseudo-random sequence generators 15 and 23 producing the same pseudo-random sequence and being synchronised, the necessary synchronisation can be easily arranged and so need not be described in detail, so that the numbers supplied to the code selector 14 and to the code selector 22 along line 25A are the same. The code selectors 14 and 22 have the same clock pulse sequences stored at equivalent addresses and use the same algorythm to derive addresses from the numbers provided. The algorythms can be changed depending on the time, who the recipient of the message is, or in any other predetermined manner, such a procedure is simple and ned not be discussed here.

The code selector 22 controls variable divider 21A to read the encrypted signal into register 19A at the same time it was read out of register 11. A counter 26 counts

the number of clock pulses sent to the register 21A and signals the code selector 22 along line 27A, every 1024 poulses. When the code selector 22 receives a signal on line 27A it changes the output of variable divider 21A to the next clock frequency.

After 4096 clock pulses, counter 26 signals switches 24 and 30 along line 31. In response to this signal, switches 24 and 30 change position so that shift register 19A is connected to the output of the decrypting system 9, and shift register 19B is connected to the input. Counter 26 also signals the pseudo-random code generator 23 along line 29, in response to this signal the pseudo-random code generator 23 steps to its next setting and provides this number to the code selector 22 along a line 25B, it also provides the number two steps before this number in the pseudo-random code sequence to the code selector 22 along the line 25A.

The code selector 22 uses these two numbers to find two memory addresses and obtains two series of clock rates. The series of clock rates found using the present number from the pseudo-random code generator 23, which will be the same as the series being used to clock encrypting register 11, are used by code selector 22 to clock the signal received by the receiver 18 into the shift register 19B. The series of clock rates found using the two steps back number from the pseudo-random generator code generator 23, which will be the same as the series

which was used to read the data now in shift register 19A out of shift register 11, are used by code selector 22 to clock out the data in register 19A to an output 32 of the decrypting unit 9.

The counter 26 separately counts the number of clock pulses going to registers 19A and 19B and signals the code selector along lines 27A and 27B respectively every 1024 pulses on the appropriate line. Every 4096 pulses the counter signals the code selector 22 on line 28. Note that since all code series used produce 4096 pulses in 58.368 msec. the counts of pulses to both registers will reach 4096 simultaneously. When the code selector 22 receives a signal on line 27A it sets variable divider 21A to produce the next clock frequency in the series used to clock the register 19A, and similarly when it receives a signal on line 27B, it sets variable divider 21B to produce the next clock frequency in the series used to clock the register 19B.

Thus encrypted data is read into register 19B at the same series of frequencies it was read out of encrypting register 11, and the data that was previously read into register 19A at the same series of frequencies as it was read out of encrypting register 11 is read out of register 19A at the same series of frequencies as it was read into register 19A and is decoded.

At the end of 4096 clock pulses register 19A is empty and register 19B is full, the switches 24 and 30 are

changed to connect register 19A to read in data and register 19B to read out data and the pseudo random sequence generator 23 is stepped. Encrypyted data from encrypting register 11 is then fed into register 19A while the data in register 19B is read out in decrypted form. This cycle of use of the two registers 19A and 19B then continues with the lines alternately reading in and reading out data and providing a continuous decrypted signal at output 32.

The system described could be made more secure by removing the constraint that each clock frequency in each series of clock frequencies lasts for the same number of pulses, this would allow a very much larger number of possible series to be used. However, it would then be necessary for the code selectors 14 and 22 to programme counters 16 and 26 respectively with the number of pulses that each frequency in each sequence of frequencies would last so that the code selectors 14 and 22 could be signalled to alter the clock frequencies at the right times.

The system could be made still more secure by arranging the encrypting and decrypting shift registers to be of variable length. All the shift registers would have to change their length simultaneously of course. Such a change could not be made while data was being passed through the system without seriously degrading the output signal, but it could be carried out during silent parts of

the signal, silences being common in speech. A system with this facility would need a sensor in the encrypter to detect silences or blanks in the incoming signal and some means to inform the decrypter what the new register length was. It would also be necessary to alter the clock frequency series produced by selectors 14 and 22 to fit each new register length.

Also the signal to be transmitted could be pre-encrypted and post decrypted by another similar encryption/decryption system, or indeed by any other type of encryption/decryption system.

CLAIMS

1. A data encryption/decryption method, in which: first and second registers are associated with encryption and a third and fourth with decryption; plain-form data is transferred sequentially through the four analogue shift registers such that each data element is clocked at different clocking rates and for each register data which is fed in at one clocking rate is then fed out at another and data is fed into the third register at the same clocking rate as it was fed out of the second register, and is fed out of the third register at the same clocking rate as it was fed into the second register; and data is fed into the fourth register at the same clocking rate as it was out of the first register and is fed out of the fourth register at the same clocking rate as it was fed into the first register whereby, by virtue of the resulting frequency shifting, the data transferred between the two pairs of registers is encrypted, but when fed out of the fourth register is decrypted, and in plain form.

2. A method as claimed in claim 1, in which the clock rates for the third and fourth registers are not the same as, or are not in synchronisation with, those of the first and second registers.

3. A method as claimed in any of the preceding claims, in which, to synchronise the application to each register of the appropriate two different sets of clock pulses, each of the two pairs of registers have their own,

nominally independent, clock pulse source, each pulse source is associated with trigger pulse transmitting/receiving means, such that the encrypting register pair's timing system can send to the decrypting register pair's timing system a suitable trigger pulse at some appropriate time, and that pulse can be caused to re-trigger the decrypting register's clock, and place the two clocks in perfect synchronisaton.

4. A method as claimed in any of the preceding claims, in which, to raise the security level, either the four clock rates are slowly modified according to some pre-agreed code, or the clock pulse trains are themselves modified in a prearranged manner.

5. A data encryption/decryption method in which a first register is associated with encryption and a second and a third register are associated with decryption; plain form data is fed into the first register at a series of clock rates and then fed out of the first register at a different series of clock rates and fed into the second register at the same series of clock rates it was fed out of the first register at, when the second register is full the data being fed out of the first register is fed into the third register at the same series of clock rates it was clocked out of the first register at and the data in the second register is fed out at the same series of clock rates it was fed into the first register at, when the third register is full the data being fed out of the

first register is fed into the second register at the same series of clock rates it was fed out of the first register at and the data in the third register is fed out at the same series of clock rates it was fed into the first register at, and this cycle of use of the second and third registers is repeated; the series of clock rates supplied to the registers being such that; data transferred between the first register and the second and third registers is encrypted, and the data output of the second and third registers is plain form and the duration of time taken to fill or empty each of the registers with data is a constant.

6. A data encryption/decryption method as claimed in claim 5 in which the first, second and third shift registers are all of equal capacity and the duration of time taken to fill or empty each of the registers with data is the same.

7. A method as claimed in any preceding claim in which the data is speech.

8. A method as claimed in any of the preceding claims, wherein each shift register is a charge coupled device (CCD).

9. A method as claimed in any preceding claim, in which data is pre-encrypted by one or more extra registers before being supplied to the encrypting register or registers and is post-decrypted by one or more extra registers after coming out of the decrypting registers.

10. Data encryption/decryption equipment, which includes: four shift registers arranged in a sequence; tranception means whereby the output of the second register can be supplied to the input of the third register, input means for feeding plain form data to the first register; output means for feeding plain form data from the fourth register; clock pulse means for each register, for giving a sequence of different clock signals to the registers to control the transfer of their contents therethrough; and synchronisation means enabling the clock pulse means for each register to be synchronised one with the other, such that, when plain form data is transferred sequentially through the four registers at four different clocking rates, (a) for each register, data which is fed in at one clocking rate is then fed out at another, (b) data is fed into the third register at the same clocking rate as it was fed out of the second register, and is fed out of the third register at the same clocking rate as it was fed into the second register, and (c) data is fed into the fourth register at the same clocking rate as it was fed out of the first register, and is fed out of the fourth register at the same clocking rate as it was fed into the first register.

11. Data encryption/decryption equipment which includes: a first shift register associated with encryption and a second and a third shift registers associated with decryption; tranception means whereby the output of the

first register can be supplied to the inputs of the second or third registers; input means for feeding plain form data to the first register; output means for feeding plain form data from the fourth register; clock pulse means for each register for giving a sequence of different clock signals to the registers to control the transfer of their contents therethrough: synchronisation means enabling the clock pulse means for each register to be synchronised one with another; and switching means enabling sections of the output of the first register to be supplied alternately to the inputs of the second and third registers, each section being one register full of data, arranged such that when plain form data is transferred through the register at a plurality of different clocking rates, for each register data which is fed in at one clocking rate is fed out at another, data is fed into the second register at the same rate as it was fed out of the first, data is fed out of the second register at the same rate it was fed into the first, data is fed into the third register at the same rate it was fed into the first and data is fed out of the third register at the same rate it was fed out of the first.

12. Data encryption/decryption equipment as claimed in claim 11 in which the first, second and third shift registers are all of equal capacity and the duration of time taken to fill or empty each of the register with data is the same.

13. Data encryption/decryption equipment as claimed in claim 11 or 12 in which said clock pulse means for each register comprise a variable divider devising clock pulses from a reference frequency source.

14. Data encryption/decryption equipment as claimed in claim 13 in which each variable divider is controlled by control means that select one of a plurality of different sequencies of different clock frequencies, which sequence is selected being decided by the output of a pseudo-random code generator.

15. Data encryption/decryption equipment as claimed in claim 14 in which which sequence of different clock frequencies is selected in response to each possible output of the pseudo-random code generator can be varied.

16. Data encryption/decryption equipment as claimed in any of claims 11 to 15 in which each clock signal in the sequence of different clock signals contains the same number of bits.

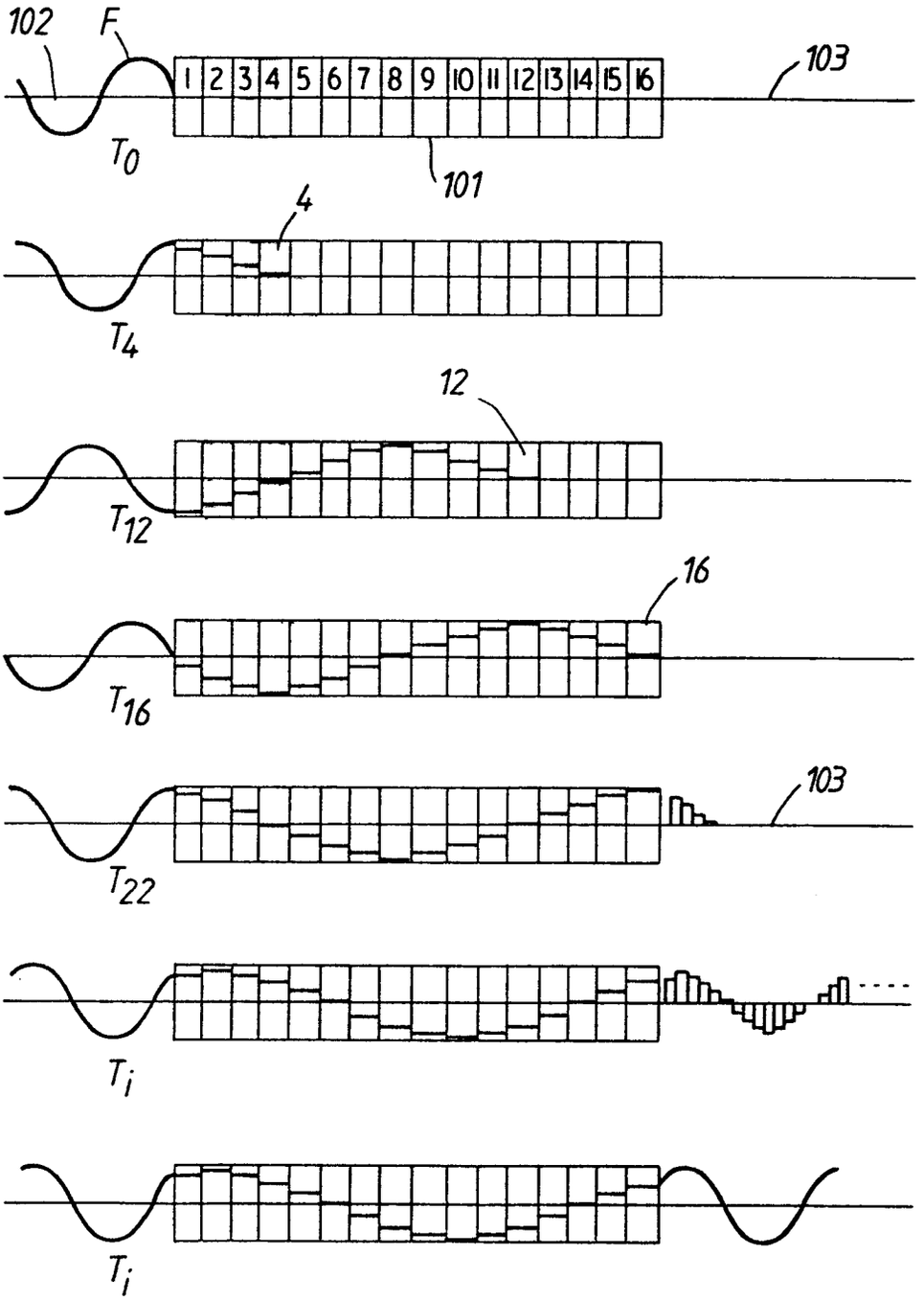

FIG. 1.

0216595

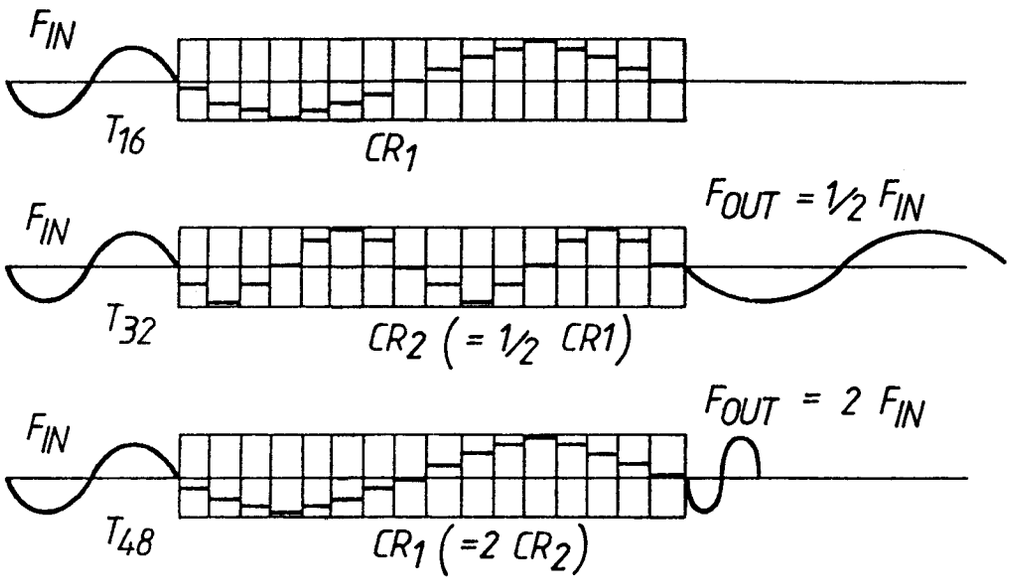

FIG.2.

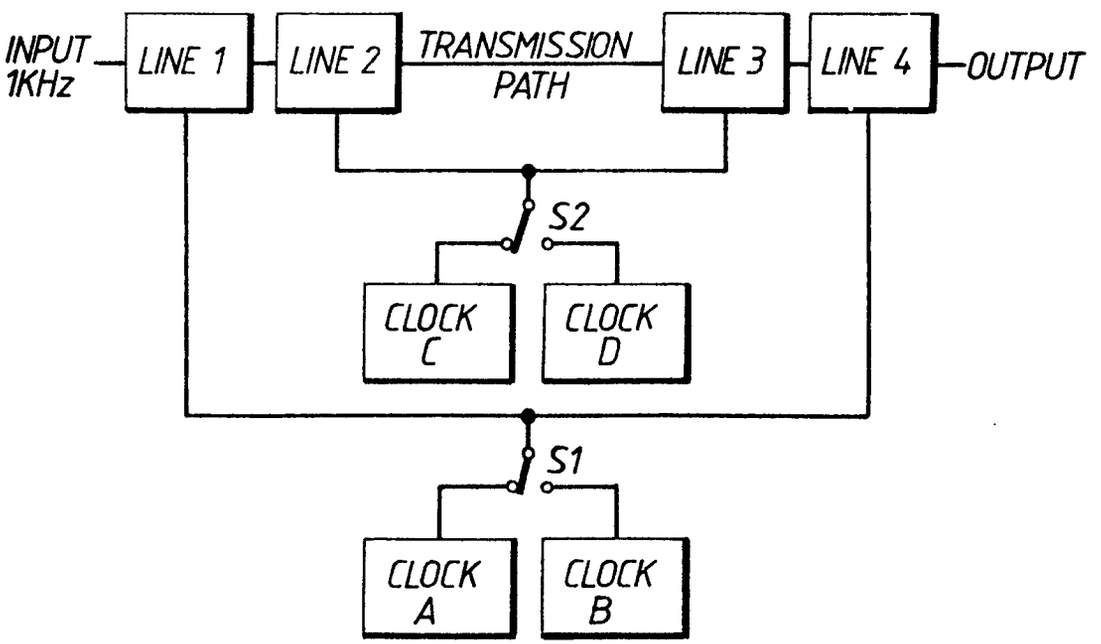

FIG.3.

0216595

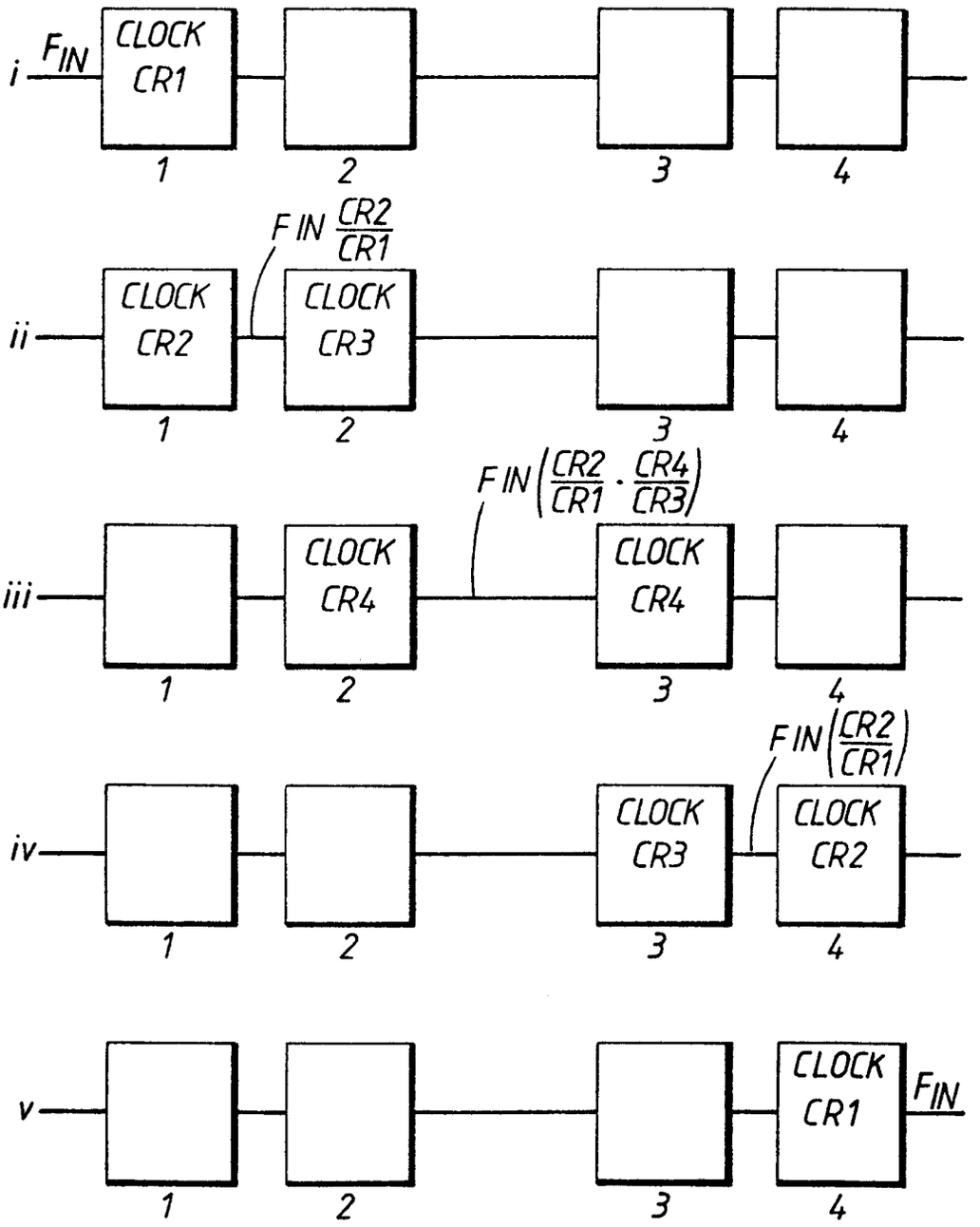

FIG. 4.

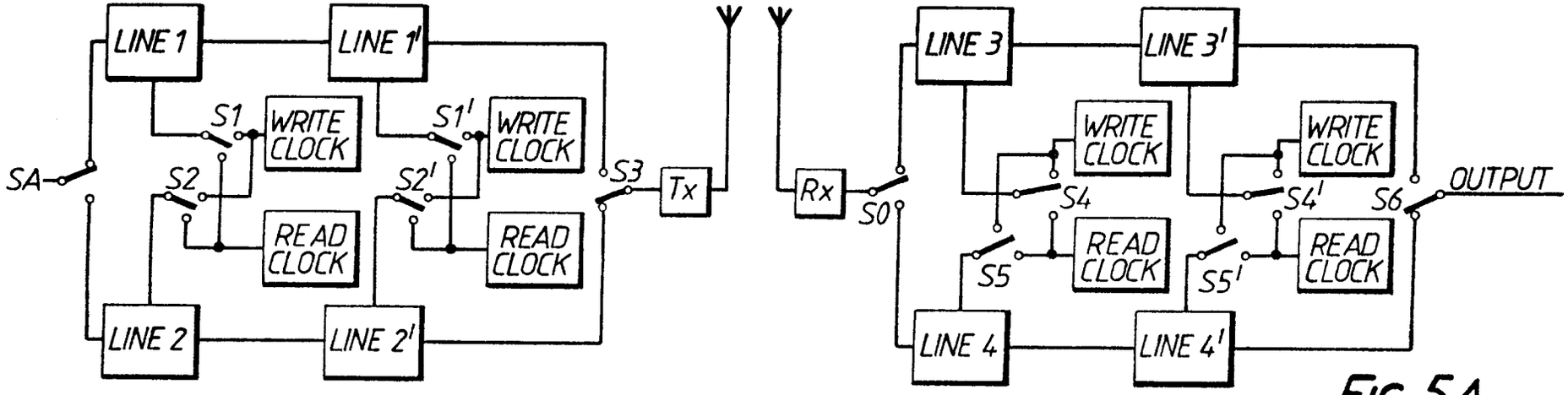

FIG. 5A.

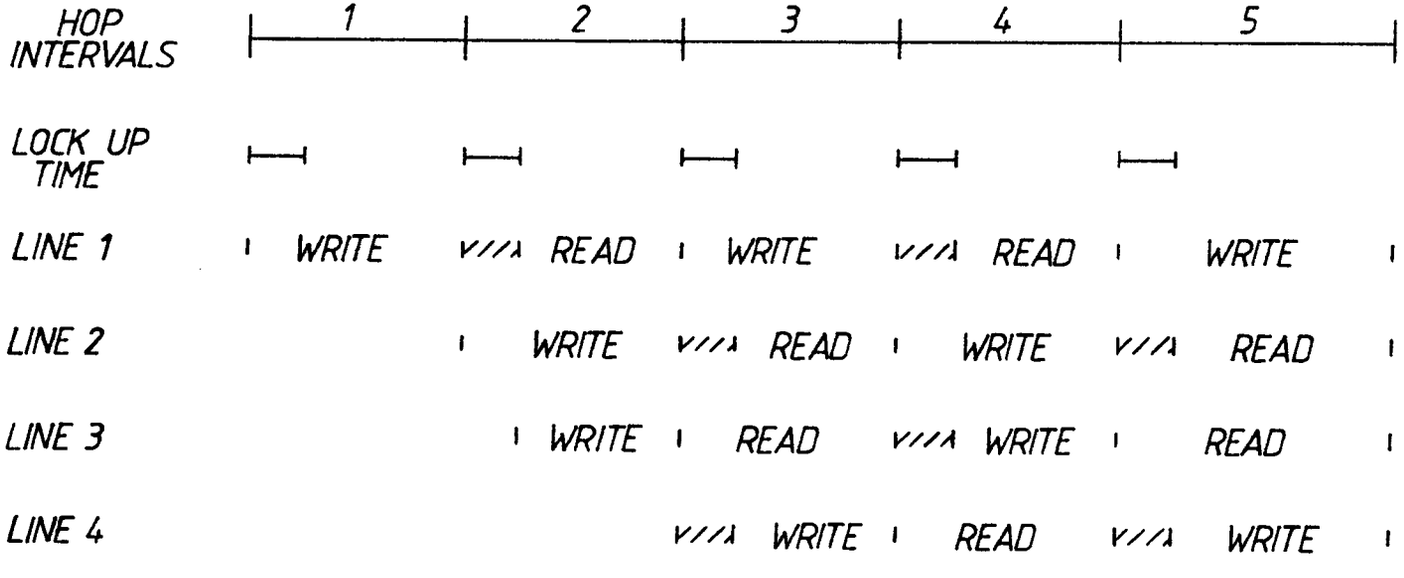

FIG. 5B.

0216595

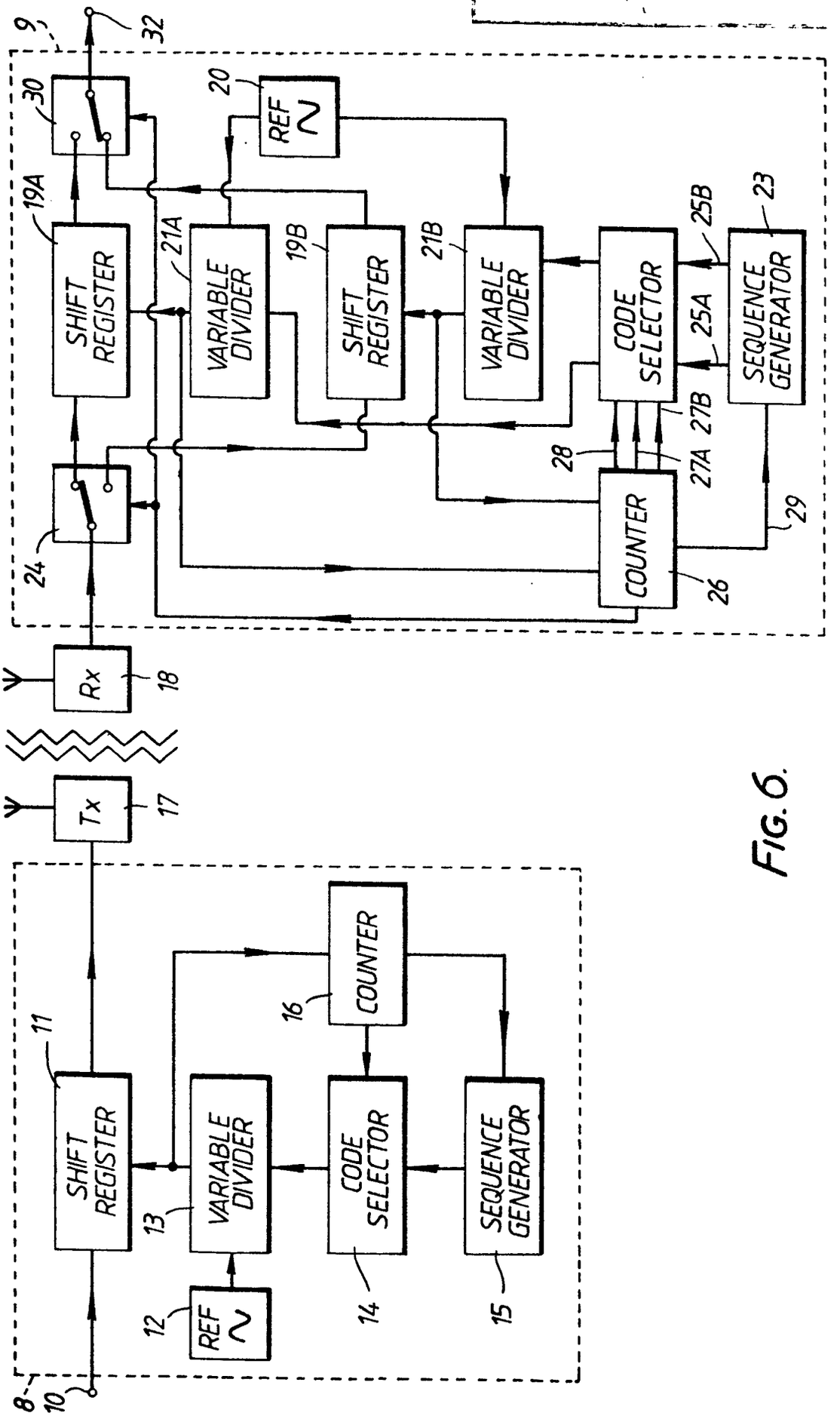
8
10
11
SHIFT REGISTER
12
REF
13
VARIABLE DIVIDER
14
CODE SELECTOR
15
SEQUENCE GENERATOR
16
COUNTER
17
Tx
18
Rx
9
32
30
24
19A
SHIFT REGISTER
21A
VARIABLE DIVIDER
20
REF
19B
SHIFT REGISTER
21B
VARIABLE DIVIDER
CODE SELECTOR
25B
25A
SEQUENCE GENERATOR
23
28
27A
27B
COUNTER
26
29

FIG. 6.