Signal encryption.

Methods and apparatus for encrypting and subsequently decrypting an analog or digital signal are disclosed. During encryption the signal waveform is transformed by a substantially continuous non-linear complex function of frequency. The transformation is characterised in that the time duration of a transformed impulse signal is substantially increased. Decryption requires transformation of the encrypted signal by substantially the complex inverse of the encryption function. The transformations may vary in time during encryption/decryption of a signal.

![Diagram](https://example.com/diagram.png)
FIELD OF THE INVENTION

The present invention relates to encryption, and in particular to a new encryption method and apparatus for encrypting a signal, and to a corresponding decryption method and apparatus for decrypting the encrypted signal so reproducing substantially the original signal.

DESCRIPTION OF THE PRIOR ART

Conventional encryption methods use bit substitution for encryption. Typically the digital data to be encrypted is combined with a random or pseudo-random sequence by modulo 2 addition. The most commonly used encryption method is the Data Encryption Standard (DES) algorithm. The complexity of this algorithm is defined by a 64-bit word which is broken down into a 56-bit cipher and 8 control bits. When using DES the data is encrypted in its digital form and is sent by conventional means such as by modulation. The encrypted data is however easily demodulated and reconverted to digital form for analysis by computer in deciphering the code.

A method for encrypting an analog signal has been disclosed in US Patent No. 2,411,683 to Guanella in which the frequency band of the analog signal is sub-divided into relatively small number of sub-bands and each of the sub-bands is delayed by a separate time delay. The encrypted signal is subsequently decrypted by sub-dividing the encrypted signal frequency band into a plurality of sub-bands and adding a complementary phase delay to each of the sub-bands. A disadvantage of this method is that the decryption process often does not result in a signal which corresponds sufficiently closely to the original signal. A further disadvantage is that when speech is encrypted the depth of encryption is often not sufficient to prevent recognition of significant portions of the speech.

Bit smearing and desmearing filters have been proposed using a constant group delay with frequency to reduce the effects of impulse noise on transmitted data. Such a system is not suitable for encryption however as the constant group delay is easily duplicated. Group delay is defined as the derivative of phase with respect to frequency, as opposed to phase delay which is defined to be phase shift as a function of frequency.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a method and apparatus for signal encryption and a method and apparatus for corresponding signal decryption.

The impulse response of the encryptor device is chosen to scramble the incoming signal which may be in digital or analog form. As a result, the encrypted signal which may also be in digital or analog form, appears noise-like, at least to an unintended cryptanalyst. The encryptor impulse response is greatly extended in time relative to an incoming impulse or signal bit, and preferably has highly irregular random variations in amplitude over its length. The magnitude and phase spectra of the transformation which is applied to the signal are then complicated non-linear functions of frequency. These spectra comprise the transfer function of the encryptor and represent the complex fourier transform of its impulse response. A suitable impulse response for the decryptor device is calculated from that of the encryptor. The respective transfer functions are essentially in complex inverse relationship.

The encryption and decryption processes are conveniently implemented by digital means in which each impulse response is represented by a finite sequence of N numbers as digital words. Typically N ranges from 128 to 4096 although longer and shorter responses are envisaged depending on the degree of security required. The encryptor impulse response defines the encryption 'key' and may be varied in time as a particular signal is encrypted, with simultaneous variations of the decryptor key. Encryption and decryption are identical processes using matched keys. An incoming digital signal is convolved with the encryptor or decryptor impulse response. An incoming analog signal is first converted to digital form using standard techniques.

A preferred embodiment of the encryptor/decryptor devices uses the circuit of a Finite Impulse Response (FIR) digital filter. Such a filter is normally used for frequency separation, particularly where special characteristics are desired such as constant group delay and sharp frequency cut off. According to the present invention however, the circuit will not be used as a filter but as an all-pass network with random magnitude and phase responses.

The present invention is an improvement over that of USSN 07/197697. The latter specification discloses an encryption system in which the the encryptor phase response is specifically chosen and from it the decryptor phase response is calculated. The respective impulse responses are
then calculated from the phase responses, both magnitude responses being constant with frequency. In contrast, the present specification discloses an encryption system in which the encryptor impulse response is specifically chosen so that both the encryptor magnitude and phase responses vary with frequency. The difficulty of calculating the decryptor impulse response in such a system has been largely overcome.

**BRIEF DESCRIPTION OF THE DRAWINGS**

Figure 1 is a schematic diagram of an N length Finite Impulse Response (FIR) digital network which may be used to implement an encryptor or decryptor according the present invention.

Figures 2a, 2b and 2c are respectively the impulse, magnitude and phase responses of a FIR digital all-pass network having zero phase and constant magnitude spectra.

Figure 3a plots a random impulse response (IR) for a 512 length encryptor according to the present invention.

Figures 3b and 3c are magnitude and phase response plots comprising part of the complex fourier transform of the IR in Figure 3a.

Figure 3d is a spectrogram of the response to an impulse of an encryptor conditioned according to Figure 3a.

Figure 4a plots the IR for a decryptor conditioned to decrypt a signal encrypted by an encryptor conditioned according to Figure 3a.

Figures 4b and 4c are magnitude and phase response plots comprising part of the complex fourier transform of the IR in Figure 4a.

Figure 5a is a plot of the overall IR of an encryptor/decryptor system conditioned according to Figures 3a and 4a.

Figures 5b and 5c are magnitude and phase response plots for the IR of Figure 5a.

Figure 6a plots a random IR for a 128 length encryptor according to the present invention.

Figures 6b and 6c are magnitude and phase response plots comprising part of the complex fourier transform of the IR in Figure 6a.

Figure 6d is a spectrogram of the response to an impulse of an encryptor conditioned according to Figure 6a.

Figure 7a plots the IR of a decryptor conditioned to decrypt a signal encrypted according to the encryptor of Figure 6a.

Figures 7b and 7c are magnitude and phase response plots comprising part of the complex fourier transform of the IR in Figure 7a.

Figure 8a is a plot of the overall IR of an encryptor/decryptor system conditioned according to Figures 6a and 7a.

Figures 8b and 8c are magnitude and phase responsive plots for the IR of Figure 8a.

Figure 9 is a block diagram showing how data encryption and decryption devices according to the present invention may be arranged.

Figures 10a-10g show typical waveforms at various points in the arrangement of Figure 9.

Figures 11a and 11b show comparative amplitude probability distributions for binary baseband data, bandwidth limited according to Figures 2b and 2c, and passed by an encryptor according to the present invention respectively.

Figure 12 is a block component diagram of an encryption system employing encryptors and decryptors according to the present invention.

Figure 13 is a block circuit diagram of an encryption or decryption apparatus to be used in the system of Figure 12.

Figure 14 represents fading in and out of an encryptor/decryptor impulse response.

Figure 15 is a vector diagram demonstrating Hilbert pair impulse responses.

Figure 16 represents fading in and out of a series of encryptor/decryptor impulse responses according to the present invention.

**DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

The present encryptor and decryptor devices are readily implemented using FIR digital filters, although they do not necessarily include filtering as part of their normal function. It is helpful however in understanding the invention to consider the network of Figure 1 with reference to FIR digital filters.


Consider a device with an impulse response as shown in Figure 2a, corresponding roughly to a typical voice grade transmission channel. The uniform magnitude and phase responses of the device transfer function are shown in Figures 2b and 2c respectively, being components of the complex
fourier transform of the impulse response. An impulse may be transmitted over such a channel with only slight distortion. Suppose however, that the impulse response takes the time-extended random form shown in Figure 3a. Corresponding magnitude and phase responses are shown in Figures 3b and 3c. An impulse transmitted over such a channel will be extremely distorted. Figure 3d shows a spectrogram or voice print for the received transmission, the blizzard-like pattern being typical of random fluctuations or noise. A signal distorted by this channel would be unrecognisable, but provided a corresponding inverse distortion could be applied, the signal content could be retrieved. The present invention provides method and apparatus by which encryption and decryption of a signal may be performed in this fashion. An encryptor and decryptor are readily implemented using FIR digital devices, although other means may conceivably be used.

The discrete impulse response (IR) of figure 3a has 512 terms, and a 512 length FIR network such as shown in Figure 1 may be conditioned to provide such a response if its h values are correspondingly set. These h-values provide the 'key' controlling the encryption process, and in general will be randomly chosen. If the resulting encryptor is presented with a series of digital words at some rate (effectively consecutive impulses), the output will consist of the sum of their separate responses staggered by time lags equal to one word length steps. This convolution of the signal and impulse response deliberately creates a high degree of intersymbol interference.

For decryption using a FIR encryptor, a complementary set of h-values are required and these may be obtained by a process which will be described later. A decryptor IR appropriate for an encryptor according to Figure 3a is shown in Figure 4a. These two responses may of course be interchanged in an encryption/decryption system. The magnitude and phase responses comprising part of the complex fourier transform of the IRs in Figures 3a, 4a are shown in Figures 3b and 3c, 4b and 4c respectively. Figure 5a shows the overall IR of an encryption/decryption system in which the IRs of Figures 3a and 4a are introduced in series. Figures 5b and 5c show the magnitude and phase response of the system which is capable of satisfactorily reproducing the original signal with only a small fixed delay.

Figure 6 shows the IR of a 128 length encryptor conditioned according to a randomly chosen set of 128 h-values. The corresponding magnitude and phase responses in Figures 6b and 6c are seen to be less complicated than those of the 512 length encryptor described above as the IR is reduced to one quarter of its previous duration. The spectrogram of Figure 6d, while still noise-like, is more regular than that of Figure 3d. Shortening the length of the encryptor will clearly reduce the security of encryption somewhat but provides improved economy and speed. In encryption of telephone quality voices the encryptor length must be sufficient to defeat the subtle perception abilities of the human ear. A 4096 length encryptor has been found to provide satisfactory security in this respect.

A decryptor IR complementary to that of Figure 6a is shown in Figure 7a. Its magnitude and phase responses are shown in Figures 7b and 7c. The impulse, magnitude and phase responses of the overall encryption channel are shown in Figures 8a, 8b and 8c, and show that reproduction of the original signal can be satisfactorily achieved with only a small fixed delay.

Figure 9 is a schematic diagram showing how the encryptor IR may be introduced into a data transmission system. The encryptor 10 is placed between the signal source 14 and the data transmission channel 16 so that when the signal is passed to channel 16 it has been scrambled by non-linear magnitude and phase shifts. At the receiving end of channel 16, a decryptor 12 is placed before the receiving equipment 18. The decryptor IR is complementary to that of the encryptor 10 so that the signal is returned to substantially its original form. The net effect of the encryption/decryption process will be a slight delay in the signal transmission time as shown by Figures 5c and 8c.

The nature of the encrypted signal differs from the unencrypted signal, and the influence of channel 16 on transmitted data is changed. For example, a signal may be temporarily disrupted while it is in the channel by sudden fading or a noise spike. This form of disruption to an encrypted signal will be averaged over a longer period of time on decryption because of the length of the decryptor IR, and is less likely to be significant, whereas information would almost certainly be lost from an unencrypted signal.

Figures 10a-10g show typical time waveforms at various points in the arrangement of Figure 9. Figure 10b shows a bandwidth limited binary baseband signal at point W in Figure 9, derived from the digital sequence represented by Figure 10a. Spreading the signal out in time at point W, synchronizing the signal to the bit rate, and providing multiple traces superimposed upon one another, produces the waveform in Figure 10c, which is known as an open 'eye' pattern. Where the signals converge at the top level, a binary 1 is detected by sampling. The bottom convergence is detected as a binary 0. The perfect convergence of these traces shows that the signal has zero intersymbol interference. At point X, the waveform has
been encrypted to that of Figure 10d. Contrasted with the waveform in Figure 10b, the encrypted data in Figure 10d has higher peaks and looks more like a noise signal. The eye pattern is also changed as shown in Figure 10e, and there is no longer an opening to the eye. At point Y the signal is unchanged from that at point X, assuming that there is no noise on the channel. However, at point Z, after decryption, the signal is restored to be the same as that at point W, as shown in Figure 10f, and the eye pattern is also restored, as shown in Figure 10g.

Figure 11a shows the amplitude probability distribution of a baseband binary random sequence, filtered to a bandwidth of B/2, where B is the bit rate, using a filter with an impulse response as shown in Figure 2a. Figure 11b shows the amplitude probability distribution for the same sequence, but the filter responses are now similar to those of one of Figures 3 to 7. The zero phase filter shows a bimodal distribution around the amplitudes of +1 and -1, whereas the non-linear filter shows a gaussian distribution about 0 amplitude. The non-linear filter produces a signal with greater entropy, and for this reason is a more efficient method of data transmission.

A major advantage of the present method of data encryption is that the bandwidth of the original signal remains unchanged. The signal simply assumes a gaussian random pattern of the same bandwidth. Another advantage is that because the impulse response of the encryptor is greatly extended in time a smearing of the signal takes place over that span of time. As a result, impulse noise and signal fades tend to have much less effect on the final signal after desmearing during encryption.

Figure 12 schematically shows an encryption system for use in a full duplex 4-wire telephone line transmission system. As the system shown is full duplex, there are two transmitter/receiver units 20 shown one on either side of the telephone line 44. The components in each of the units 20 have been given the same reference numerals to indicate that they are identical components.

Signal input 22 and output 24 are typically the microphone and speaker of a telephone handset. The combination of input analog to digital converters (A/D) 28, encryptor 30, output digital to analog converters (D/A) 32, the microprocessor controller 34 and the constants store 36 correspond to the encryption device 10 of Figure 9.

The four wire line 44 corresponds to two channels 16. A/D 38, decryptor 40, D/A 42, together with the microprocessor controller 34 and the constants store 36 correspond to the decryption device 12. The encryption and decryption devices are under the direct control of their respective microprocessors 34. When the equipment is turned on, the microprocessors 34 load encryption and decryption key values (equivalent to the h-values of a FIR digital filter) into the encryptors 30 and decryptors 40. These constants are stored in some medium such as EPROM, magnetic tape of disc 36.

The above describes a 4-wire telephone line system. In the case of a 2-wire line as would normally be used for an all digital system, the transmission and receiving channels are the same, connected by hybrid to each unit 20 as is well known. A/Ds 28 and 38 become serial-to-parallel converters (S/P) although S/Ps 28 may be unnecessary if the data is already available in parallel form.

Present encryption devices according to the invention satisfactorily use 2048 and 4096 length encryptors, although considerably shorter lengths are envisaged. The keys are stored in EPROMs accessed by a microprocessor-controller. Several separate keys are stored for each of encryption and decryption. Switching keys involves adjusting a dip-switch located inside the device. This design will be described with reference to Figure 13 and is equally applicable to a decryption device. Complementary devices comprise essentially the same circuitry.

Although the pre-stored method of key control is sufficient at present, it may be necessary in some cases to transmit new keys with which the system will be programmed. Such transmissions may themselves by encrypted by independent means. Ultimately, it may be desirable to enlarge the capabilities of the microprocessor-controller, to give it the capability of calculating keys independently, with the keys being changed by local command, timing or other means.

In a preferred embodiment, the keys to the encryptor and decryptor each consist of 2048 16-bit words while the encryptor input data consists of 13-bit words. Shorter keys may be implemented through software modifications. Short lengths are desirable for increased speed of the system, and in many applications the apparatus hardware may be connected for short lengths only.

Figure 13 lays out schematically a design for the preferred embodiment. An input analog-to-digital or serial-to-parallel converter 28 or 38 converts the incoming signal into discrete samples, say 12 to 14 bit words. These are placed in a delay line formed by DATA ram 210. A static memory, COEFF ram 218 contains the h-values which determine the impulse response. Connected to these two is a multiplier accumulator (MAC) 220. This device 220 takes each sample in the delay line (2048 steps in this case), multiplies each by their respective h-value, adds all together, and finally gives an output sum to the output digital-to-analog or parallel-to-series converters 32 or 42.
At this point a new sample comes from the converter 28 or 38, and the process of addition and accumulation is repeated for another 2048 steps to obtain the second output, and so on. The MAC 220 has to work 2048 times as fast as the converter 28 or 38 and converter 32 or 42.

**OPERATION OF ENCRYPTOR**

When the encryption device is switched on or reset, a set of 2048 h-values (Hj) selected by the coefficient selector 242 is transferred to the COEFF ram 218. An initial set of 2048 DATA values (Xk) is read into the DATA ram 210 from the input converter 208. These values may be samples of the analog signal to be encrypted. In encryption of an already parallel digital signal, the A/D or S/P converters may be dispensed with.

MAC 220 then calculates the product of each of the corresponding pairs (Hj*Xk) and accumulates the sum of these products to calculate the value for the encrypted signal (Y). Hence the signal is given by:

\[
Y = \sum_{i=0}^{2047} H_i \times X_i
\]

The next data value X is then read into the DATA ram 210 as Xo. Data values Xo to X2046 become Xi to X2047 and the previous value of X2047 is dropped. The value of Y for this new set of data values (Xk) is then calculated. Thus a cycle of 2048 multiplications is performed for each Y-value output.

**CIRCUIT DESCRIPTION**

The encryption device 200 (Figure 13) comprises two main blocks, an encryptor block 202 and a coefficient loading block 204. The encryptor block is connected to the output latch of analog-to-digital or serial-to-parallel converter 208 by a 13-bit DATA data bus 248. Counter controller 214 controls the DATA and COEFF counters 212 and 216 are modulo 2048 binary counters, the binary outputs of which are connected to the address inputs of DATA and COEFF rams 210 and 218 respectively. DATA ram 210 contains 2048 13-bit words which may represent samples of an analog input signal or words of an originally digitized signal. COEFF ram 218 contains 2048 16-bit words which represent the h-values of the encryptor. The 2's complement representation of integers is used throughout the encryption device.

Multiplier/accumulator (MAC) 220 has two input registers (not shown) one connected to the DATA data bus and the other to the COEFF data bus. The output of MAC220 is connected to a 12-bit latch 222 which forms the encrypted data output for the encryption device 200. Latch 222 is connected to the digital-to-analog or parallel-to-serial converter 224.

In one embodiment, the MAC 220 is a Wafer-scale Integration WS59510 or a General Electric Intersil IM29C510 multiplier/accumulator. In both cases the MAC has a 36-bit internal register for storing the sum of the products Y. The output is configured to give a 12-bit output by taking the 12 most significant bits of the value for Y.

Coefficient leading block 204 is used to load a selected set of h-values into the encryptor when the device 200 is switched on or re-initialised. The coefficient loading block 204 is controlled by a microprocessor 232 which has an output line 238 connected to the chip select of EPROM 226. In the prototype, EPROM 226 contains 16 sets of 2048 h-values for the encryptor, although many more sets may be necessary in high security applications of the invention. In the prototype, coefficient selector 242 is a four switch dip-switch set to a given position, address bits 0-15 of the EPROM address the 2048 h-values in a selected set.

Microprocessor 232 (Figure 13) also has control line 240 going to the clock input of COEFF counter 216, and control line 252 going to the read/write input of COEFF ram 218. Bi-directional three-state buffer 228 is used to isolate the coefficient loading block from the encryptor block during each cycle of the device 200 and to allow data transfer, to and from COEFF ram 218, from and to the microprocessor 232 respectively, during coefficient loading. BUFFER 230 is used to transfer the 16-bit COEFF data to an 8-bit port of the microprocessor 232.

**NORMAL OPERATION**

During normal operation of the encryption device 200, DATA ram 210 contains 2048 samples of the input signal and COEFF ram 218 contains the 2048 h-values comprising the encryptor key. The internal accumulator 221 of the MAC 220 is zeroed (ie. PRODUCT = 0) at the beginning of each cycle.

DATA counter 212 and COEFF counter 216 contain initial values D0 and C0 respectively which appear on the DATA address bus 244 and the COEFF address bus 246 respectively. D0 addresses data element Xo in DATA ram 210 and C0
addresses coefficient element \( H_0 \) in COEFF ram 218 causing \( X_0 \) to appear on DATA data bus and \( H_0 \) to appear on COEFF data bus 250. MAC 220 reads in the values \( X_0 \) and \( H_0 \) calculates their product \((H_0'X_0)\) and adds this to the running total PRODUCT stored in the internal accumulator 221 of MAC 220. This completes the 0th step of the one cycle of encryptor 202. As PRODUCT was set to zero before the cycle began, PRODUCT now equals \( H_0'X_0 \).

The next step of encryptor 202 begins and counters 212 and 216 are incremented (modulo 2048) to the values \( D_i \) and \( C_i \) causing \( X_i \) and \( H_i \) to appear on the DATA and COEFF data buses respectively. MAC 220 then calculates \( H_i'X_i \) and adds this to PRODUCT. This process is repeated for 2048 steps.

In general, during the ith step of encryptor 202, DATA counter 212 contains \( D_i \) and COEFF counter 216 contains \( C_i \), causing \( X_i \) and \( H_i \) to be addressed in DATA ram 210 and COEFF ram 218 respectively. \( X_i \) and \( H_i \) subsequently appear on the DATA and COEFF data buses 248 and 250 respectively. MAC 220 calculates \( H_i'X_i \) and adds this to PRODUCT.

At the end of the cycle, \( i=2047 \) and PRODUCT is given by:

\[
\text{PRODUCT} = \sum_{i=0}^{2047} H_i'X_i
\]

PRODUCT is then scaled to give a 12-bit signed integer \( Y \). \( Y \) is loaded into product latch 222 which is clocked at an appropriate time to the output converter 224.

After the end of step 2047, DATA counter 212 is incremented by counter controller 214 to the previous value of \( D_0 \). Counter controller switches read/write line 234 to read. Digital input circuit 208 at this time now has the next DATA value available and this is read into DATA ram 210 at the location addressed by \( D_0 \). DATA counter 212 is incremented again so that the new value of \( D_0 \) is the same as the previous value of \( D_1 \). COEFF counter 216 is also incremented by one to \( C_0 \) by the counter controller 214. This value of \( C_0 \) is the same as that used previously. Counter controller switches read/write line 234 to write and the internal accumulator 221 of MAC 220 is zeroed. The encryptor is now ready to begin another cycle although ideally, a new key could be loaded at this stage.

When the encryption apparatus 200 is switched on or is reset microprocessor 232 causes a selected set of 2048 h-values stored in EPROM 226 to be loaded into the COEFF ram 218.

EPROM 226 contains 16 blocks of 2048 16-bit words which are 16 sets of h-values for the encryption apparatus 200. The set of h-values to be used is selected by the coefficient selector 242 which in the prototype is merely a dip-switch with four switches. The four switches are connected to address bits 11-14 of the address input to EPROM 226 so that sixteen different sets of h-values can be stored in the EPROM in consecutive 2048 16-bit word blocks.

Microprocessor 232 zeros COEFF counter 216, switches buffer 228 to allow data transfer from EPROM 226 to COEFF ram 218, sets read/write line 252 to read, switches buffer 230 to allow data transfer from EPROM 226 to the microprocessor 232 and enables EPROM 226 via chip select line 238. The contents of memory location 0 in EPROM 226, which corresponds to \( H_0 \), are then transferred to memory location 0 in COEFF ram 218 and to the microprocessor 232. The value of \( H_0 \) is stored by the microprocessor 232 as the first addend in a 16 bit checksum. Counter 216 is then incremented to 1, and memory location 1 in EPROM 216, which corresponds to \( H_1 \), is transferred to memory location 1 of COEFF ram 218 and added to the checksum in microprocessor 232.

In general, during write step \( i \) microprocessor 232 increments COEFF counter 216 from \( i-1 \) to \( i \), and the contents of memory location \( i \) in EPROM 226, which corresponds to \( H_i \), are written into memory location \( i \) of COEFF ram 218 and added to the checksum in microprocessor 232. The process continues until all 2048 h values \((i=2047)\) have been read into COEFF ram 218, and the checksum has been completed. Microprocessor 232 then disables EPROM 226 via chip select line 238, sets read/write line 252 to write, and switches buffer 228 to allow data transfer from COEFF ram 218 to microprocessor 232.

COEFF counter 216 is then stepped until all 2048 locations in COEFF ram 218 have been read back into microprocessor 232 and added to form a further checksum. The two checksums are compared and if equal, the encryption device 200 is set in normal running mode. EPROM 226 is then deselected and buffer 228 is disabled. DATA ram 210 is initialized by performing 2048 steps preferably without any \( Y \)-values being output. if the checksums are not equal, an LED on the device indicates to the user that a memory fault has been detected. The coefficients may be reloaded with a further memory check, although encryption will not proceed until such memory faults have been cleared. It is preferably that the coefficients of
Encryption and decryption devices will operate in the following fashion:

(a) Turn equipment on.
(b) Wait for warm-up and loading of keys.
(c) Equipment is now ready to send and receive. In one embodiment of the invention, improved encryption security may be provided using the apparatus of Figure 13 by 'rolling' the encryptor through two or more impulse responses during transmission of a signal. This process can be carried out in accordance with a time sequence which is synchronised between the transmitting encryption device and the intended recipient decryption device. The time sequence can provide for linear or random rates of change between various impulse responses. This technique has been simulated by computer and found feasible for encryption of both analog and digital signals.

The coefficient loading circuit 204 remains active during operation of the encryption device and modifies the coefficients used by the encryptor 202 once signal transmission proceeds. The coefficients held in COEFF ram 218 are renewed by microprocessor 232 during encryption. The time sequence controlling the coefficient variation is held in additional memory (not shown in Figure 13) to which the microprocessor has access. For example, the coefficients may be renewed after each cycle of MAC 220, that is, after each Y value is output to the converter 32 or 42. The microprocessor 232 must then work at least as fast as MAC 220 which in turn must work 2048x as fast as the converter 28 or 38. The microprocessors of the encryption and decryption devices must clearly be synchronised for proper decryption to occur, and this is easily ensured by transmission of suitable timing signals during startup of an encrypted transmission.

In the rolling process, 'fade in' and 'fade out' of the preferably random IRs may be performed by considering consecutive IRs to be additive as uncorrelated signals, just as 2 independent noise sources are uncorrelated. That is, because of the random phase relationship between uncorrelated impulse responses, they must be combined during the fading process by power rather than voltage additions.

The spectrum of an impulse response which varies in time is shifted by an amount which depends on the rate of variation. Experimentally, shifts of up to ±100Hz have so far been simulated in transmission over a voice channel and are found to give negligible effect on the quality of the signal. Consecutive IRs are faded in and out of the encryptor and decryptor according to Figure 14, in which X and Y represent contributions to the signal generated by the fading in and fading out responses respectively. Their combined power should remain constant during the process, as is evident from the figure. An unintended cryptanalyst will thereby be less likely to be able to determine when and how the variation in encryptor IR is taking place. Also, the rate of variation must be sufficiently slow that the shift in the spectrum of the IR and therefore in the spectrum of the transmitted signal remains 'small'. As mentioned, through computer simulation shifts of up to at least 100Hz have been found acceptable, compared with the 10^4Hz A/D sampling rate for encryption of a voice signal.

When the phase angles of all components of a signal are shifted by ±90 degrees, the resulting function of time is known as the Hilbert Transform of the signal (see "Communication Systems" S Haykin, Wiley, 1978). Two signals which are related by Hilbert Transform are referred to as a Hilbert Pair. A Hilbert Transform exists for any signal, and any IR, including the random IRs used in the present invention. The Hilbert transform for any of these IRs may be derived using well established software means.

Varying the encryptor IR between each of a Hilbert pair of IRs is analogous to changing the phase of a vector as indicated in Figure 15. The magnitudes of vectors R and H correspond to the amplitudes of each IR (i.e. particular h-values) of the Hilbert pair. Varying the phase angle P by ΔP in time interval Δt gives a rate of change of phase shift ΔP/Δt to the IR, which implies a frequency shift, and the entire spectrum of the signal is shifted up or down by a known amount. Hilbert pairs complementary to those of the encryptor are stored in the decryption device and a corresponding IR variation takes place as signal transmission proceeds. According to Figure 15, the coefficients of the encryptor IR (and simultaneously the synchronised decryptor IR) may be calculated as: RcosP + HsinP. These coefficients are to be calculated by the microprocessor 232 and installed in the COEFF ram 218 between cycles of the encryptor 202.

The transitional encryptor and decryptor IRs calculated during the variation between known matched, Hilbert pairs of IRs have been found to be sufficiently well matched that acceptable signal encryption/decryption takes place during the fading process.

In the above discussion, it was assumed that the two encryptor IRs (and corresponding decryptor IRs) in question constitute a Hilbert pair, so that the resultant signal is effectively phase shifted in time, in a predetermined manner. This rate of change may be constant with time, so that the vector in Figure 15 continues to rotate in one direction, causing a positive or negative continuous
frequency shift of the signal. Alternatively, the rate of change of phase may be random with time, resulting in a fluctuation in frequency which is both positive and negative with time, depending on the sign of the random time sequence.

Recent simulations have indicated that consecutive IRs do not in fact have to be components of a Hilbert pair but may be two totally uncorrelated impulse responses. In this case it may be more desirable to perform a simple constant rate of change of IR with time, continuously fading in and fading out through a series of predetermined responses stored in the EPROM 226, as shown in Figure 16.

Returning now to the impulse responses of the encryption and decryption devices. In order to decrypt a signal, a satisfactory 'inverse' IR to the proposed encryptor IR must be known. In order to obtain each matching pair of impulse response (i.e. two complementary sets of h-values), a numerical technique is presently employed in which an initial set of h-values are successively modified. According to this technique the encryptor and decryptor h-values may be determined as follows:

1. An initial set of h-values is chosen for the encryptor. In the embodiment previously discussed there are 2048 16-bit random numbers in the set, normalised say between +1 and -1. These define an initial highly irregular piecewise IR.

2. The complex fourier transform of the initial IR is now obtained, in practice by Fast Fourier Transform. The magnitude and phase components of this transform are highly irregular functions of frequency and are normally deliberately truncated, sat at the aliasing frequency of the A/D converter of the encryption device. In the embodiment of Figure 12, which is intended for transmission over a voice grade channel, the A/D sampling frequency is approximately 10 kilohertz and the aliasing frequency is therefore approximately 5 kilohertz. Modifications of the transform may of course vary depending on the form of the transmission channel.

3. The Fourier transform obtained in step 2 is "inverted". If a point on the transform has magnitude A and phase P, then the corresponding point on the inverse transform is given magnitude 1/A and phase -P. This new complex function is a first approximation to the fourier transform of a possible decryptor IR.

4. The first approximation IR of the decryptor is obtained by Fast Fourier Transform. Because the amplitude inversion operation of step 3 is non-linear, this first approximation IR is normally longer than that of the encryptor and is truncated to be equal in length. In the prototype this length consists of 2048 suitably scaled 16-bit h-values.

5. The two sets of h-values, one for the encryptor and one for the decryptor, must be complementary or matched in order than an encrypted signal can be returned to substantially its original form. Due chiefly to the necessary truncation procedures, the initial and first approximation h-values determined by the above process will not usually be a satisfactory match. A better match may often be obtained by repetition of the above process, the first approximation h-values being substituted for the initial values of step (1). After a sufficient number of repetitions, the initial and final values of the last iteration may provide the impulse responses of a complementary encryptor/decryptor pair. Reducing the length of the encryptor actually reduces the success rate of the matching process. For example, for a 2048 length encryptor, the rejection rate (poor encryptor/decryptor match) after 300 iterations is less than 5% while that for a 128 length encryptor is about 65%.

Alternatives to the iterative process undoubtedly exist, such as Wiener Filtering, and these are presently being investigated. They will allow easier determination of decryptors for shorter length encryptors. The signal delay and cost of an encryptor are proportional to its length and therefore shorter length encryptors are preferable, provided sufficient encryption security can be achieved.

Approaching the encryption system from a cryptanalyst's point of view requires a complete reorientation of thinking with regard to that of conventional cryptanalysis. The reason is that now the cryptanalyst no longer has simple random binary numbers to sort out. Rather, he has a complete set of complex binary words representing voltage levels, which have not yet been resolved into random binary numbers. This is because of the closure of the eye pattern. Worse still, with analog transmission of the encrypted signal, he cannot even demodulate the waveform until he has sorted out these complex words.

Using the example of a 2048 length encryptor, with each h-value represented by 16 binary bits, the probability of guessing all bits correctly is one part in 2^2048x16 which clearly makes the cryptanalyst's task formidable if not impossible.

Claims

1. A method of encrypting a signal comprising, applying a frequency dependent transformation to the waveform of the signal, said transformation being a substantially continuous non-linear complex valued function of frequency over a finite bandwidth, the functional form of said function being selected to substantially increase

2. A method of encrypting a signal comprising, applying a frequency dependent transformation to the waveform of the signal, said transformation being a substantially continuous non-linear complex valued function of frequency over a finite bandwidth, the functional form of said function being selected to substantially increase...

3. A method of encrypting a signal comprising, applying a frequency dependent transformation to the waveform of the signal, said transformation being a substantially continuous non-linear complex valued function of frequency over a finite bandwidth, the functional form of said function being selected to substantially increase...

4. A method of encrypting a signal comprising, applying a frequency dependent transformation to the waveform of the signal, said transformation being a substantially continuous non-linear complex valued function of frequency over a finite bandwidth, the functional form of said function being selected to substantially increase...
the time duration of an impulse encrypted by the method relative to the time duration of an impulse bandwidth limited by said finite bandwidth.

2. A method of decrypting a signal encrypted by the method of claim 1 comprising, applying a frequency dependent transformation to the waveform of said encrypted signal, said transformation being a substantially continuous non-linear complex values function of frequency over a predetermined finite bandwidth, the functional form of said function being substantially the complex inverse of the function used in the encryption method of claim 1.

3. Apparatus for encrypting a signal comprising, transformation means for transforming the waveform of the signal, the transformation means being conditioned such that said waveform is transformed by a substantially continuous non-linear function of frequency over a finite bandwidth, the functional form of said function being selected to substantially increase the time duration of an impulse encrypted by the apparatus relative to the time duration of an impulse bandwidth limited by said finite bandwidth.

4. Apparatus for decrypting a signal encrypted by the apparatus of claim 3 comprising, transformation means for transforming the waveform of said encrypted signal, said transformation means being conditioned such that said waveform is transformed by a substantially continuous non-linear function of frequency over a predetermined finite bandwidth, the functional form of said function being substantially the complex inverse of the function used in the apparatus of claim 3.
(a) Impulse Response

Magnitude Response

(b) Phase Response

FIG. 2a

FIG. 2b

FIG. 2c
FIG. 3a

IMPULSE RESPONSE

FIG. 3b

MAGNITUDE RESPONSE (dB)

FIG. 3c

PHASE RESPONSE
FIG. 3d
FIG. 5a

**IMPULSE RESPONSE**

-0.5

-1.0

-1.5

0.0

0.5

1.0

1.5

TIME (ms)

FIG. 5b

**MAGNITUDE RESPONSE (dB)**

-1.5

-1.0

-0.5

0.0

0.5

1.0

1.5

1000 2000 3000 4000 5000

FREQUENCY (Hz)

FIG. 5c

**PHASE RESPONSE**

0 1 2 3 π

0 1 2 3 π

1000 2000 3000 4000 5000

FREQUENCY (Hz)
FIG. 8a

IMPULSE RESPONSE

FIG. 8b

MAGNITUDE RESPONSE (dB)

FIG. 8c

PHASE RESPONSE
FIG. 1

FIG. 9
FIG. 10a

FIG. 10b

FIG. 10c

FIG. 10d

FIG. 10e

FIG. 10f

FIG. 10g

FIG. 11a

FIG. 11b