
Method and device for speech encryption and decryption
in voice transmission

Description

The invention relates to a method and a device for speech encryption and decryption in voice transmission and in apparatuses for voice transmission which are equipped with a front-end unit for digitizing a voice signal and matching a transmitted signal to a predetermined transmission channel on the one hand and/or for digitizing a received signal and for matching the conditioned received signal to a voice reproduction device on the other hand.

Reference is made to the following known methods, which are collated like keywords, relating to the prior art for voice encryption and decryption.

1. Digitizing of voice signals, encoding of the digital values and transmission as digital data using a MODEM.
2. Storage of a sequence of the voice signal, division of the sequence into a plurality of smaller time intervals, transmission of these sub-sequences in a sequence other than the original.
3. Division of the spectral band to be transmitted into smaller sub-bands, transmission of a signal which is produced by interchanging spectral

sub-bands.

4. Frequency-band inversion, that is to say interchanging of high and low frequencies of the audio-frequency spectrum to be transmitted using a fixed or variable splitting device (mirror-image frequency method).

5. Combination of methods 2 to 4.

The known methods have the following fundamental disadvantages:

Re 1.) As a rule, the same channels must be used for the transmission of the digital data as for the unencrypted speech. Since these channels have only a limited bandwidth, data reduction methods are necessary. After reconstruction of these (reduced) data at the receiving end, it is not possible to identify the person speaking reliably.

Re 2.) For physiological reasons, the number and time duration of the sub-interval can be varied only within strict limits. This leads to it being simple to decode the transmitted signal.

The transitions between interchanged sub-intervals in general cannot be reconstructed at the receiving end in the correct phase, so that a reduction in the signal quality can be heard in comparison with the unencrypted signal.

Fundamentally, a perceptible delay exists in this method between speaking and signal transmission which, in certain types of transmission channels, leads to disturbing echo effects of the person speaking.

Re 3.) For physiological reasons, the number and bandwidth of the spectral sub-intervals are set within strict limits. This leads to it being possible to decode the transmitted signal easily. Unavoidable bandwidth overlaps of the filters required for production and

reconstruction of the sub-spectra lead to a deterioration in the transmission quality.

Re 4.) Decoding of the transmitted signal is possible with relatively little technical outlay. The residual comprehensibility of the encrypted signal is high; trained listeners can monitor transmissions even without technical aids.

Re 5.) Combinations of the various methods in general enhance the security against decryption; however, they also lead to summation of the disadvantageous properties such as deterioration of the signal-to-noise ratio and limitation to a small number of simple constellations of transmission channels.

The invention is thus based on the object of creating a method and a device for speech encryption and decryption in voice transmission which method/device can be produced in a compact manner as a module (which can also be retrofitted) and which method/device ensures considerably better security against monitoring and evaluation by third parties than the known methods and devices.

The following additional requirements for speech encryption are set in association with this object:

- Good speech comprehensibility;
- Good voice recognition;
- Little difference in quality from clear operation;
- Operation and controllability largely transparent to the user;
- Automatic recognition of encrypted signals at the receiving end;
- Capable of use in analog radio networks and in the telephone field,
- Conformity with the specified available transmission bandwidths.

The method according to the invention for speech encryption and decryption in voice transmission is characterized in that, at the transmitting end

- the digitized voice signal is converted by means of a first complex input filter having a bandwidth which corresponds to the bandwidth of the transmission channel into a complex signal which is phase-modulated by means of a code signal which is controlled by pseudo-random numbers,
- the phase-modulated voice signal is additively combined with a pilot signal, which is likewise phase-modulated in a pseudo-random distribution, to form an encrypted useful signal which is to be transmitted and
- the useful signal passes through a first complex output filter in a sequential manner together with a preamble, which is used for synchronization and useful signal equalization at the receiver end, as a complex signal, which output filter produces a real output signal which, after digital/analog conversion, is passed to a transmitted signal conditioner, and in that

at the receiving end

- the digitized received signal is converted into a complex signal by means of a second complex input filter having a bandwidth which corresponds to the bandwidth of the transmission channel,
- from this complex signal and during a preamble recognition phase, on the one hand clock synchronization for a pilot signal, which is produced at the receiver end and is phase-modulated in a pseudo-random sequence initialized by the preamble, is forced and, on the other hand, equalizer coefficients are calculated for an equalizer at the receiver end and the phase of the useful signal decryption is thus initialized,
- the encrypted useful signal is separated from its

phase-modulated pilot signal, which is superimposed at the transmitter end, by linking with the synchronized pilot signal which is produced at the receiver end, and

- the phase-modulated, encrypted digital voice signal which is thus obtained is decrypted by inverse phase modulation by means of the code signal which is produced at the receiver end and is clock-controlled by means of the preamble and, as a complex signal passes through a second complex output filter which produces a real output signal which, after digital/analog conversion, is passed to a received signal conditioner.

A viewpoint which is essential, *inter alia*, for the method according to the invention is that, after digitizing at the input side at both the transmitting end and the receiving end, complex filtering is in each case carried out, preferably by means of a Hilbert filter, which filtering produces a complex signal from a real signal, which complex signal is subjected to sampling rate reduction, the bandwidth of the respective complex filter corresponding to the reduced sampling rate. All operations which are essential for the further method then take place using the complex signals at a reduced clock frequency.

On the output side, the complex signal is preferably subjected, both at the transmitting end and the receiving end, to a sampling rate increase by insertion of zeros into the data flow. A complex filter which is in each case connected downstream, preferably likewise a Hilbert filter, is used as an interpolation filter and produces a real signal with a sampling frequency corresponding to the channel bandwidth.

A device according to the invention for speech encryption and decryption in apparatuses for voice transmission which are equipped with a front-end unit for digitizing a voice signal and matching a transmitted

signal to a predetermined transmission channel on the one hand and/or for digitizing a received signal and for matching of the conditioned received signal to a voice reproduction device on the other hand, characterized in that,

at the transmitting end

- a code generator which is controlled by a (pseudo-)random-number generator acts on a digital phase modulator which phase-modulates the digitized voice signal,
- the phase-modulated voice signal is combined with a pilot signal, which is supplied by a pilot-signal generator and is likewise phase-modulated in a random distribution, to form a useful signal,
- a preamble generator produces a preamble which is used for synchronization at the receiver end and for useful-signal equalization and is emitted sequentially and together with the useful signal, via a changeover switch which is operated in a defined clock sequence, to the front-end unit for transmitted signal conditioning, and in that

at the receiving end

- there is a digital equalizing filter for equalizing distortion of the digitized received signal, caused by the transmission channel, whose equalizer coefficients are calculated and set during the reception of the preamble,
- a device is provided for detection of the preamble within the received useful signal, which device initiates, as a function of a defined section of the preamble, the calculation of the equalizer coefficients for the equalizer filter in a higher-level computation unit and thus initializes the decryption of the useful signal by activating a clock synchronization device which, on the one hand, supplies from the received, demodulated pilot signal a control signal for sampling clock correction, by complex

multiplication by a pilot signal which is generated at the receiving end and, on the other hand, under the control of a (pseudo-)random-number generator which is likewise initialized with the clock synchronization, supplies, from the pilot signal which is supplied by the pilot-signal generator at the receiving end and via a modulator, a phase-modulated pilot signal which is linked with the equalized useful signal and is thus converted, as a phase-modulated voice signal, in a phase demodulator and controlled by the synchronized random-number generator at the receiving end, into the unmodulated, digital voice signal which is passed to the front-end unit for conversion into an audio signal.

Advantageous refinements and a development of the method and the device according to the invention for speech encryption and decryption are contained in dependent patent claims and are disclosed to the reader skilled in the art in the further course of the invention description, especially using exemplary embodiments as well with reference to the drawings, whose notes, block diagrams and the like are to be regarded as a publication essential to the invention to the same extent as the present description.

Fig. 1 shows the block diagram of a speech encryption/decryption module according to the invention, which is designated an "SE module" in the following text;

Fig. 2 shows the principle of encryption with an arbitrarily selected time profile;

Fig. 3 shows the functional block diagram of the transmitting section of the SE module;

Fig. 4 shows the principle of decryption, once again

without any reference to the correct time scale;

Fig. 5 shows the functional block diagram of the receiving section of the SE module;

Fig. 6 shows the block diagram of the signal processing at the transmitting end of the SE module;

Fig. 7 shows the structure of a (first) complex filter on the input side, preferably a Hilbert filter;

Fig. 8 shows the frequency response of the (first) complex filter on the input side, according to Fig. 7;

Fig. 9 shows the structure of a first complex output filter, preferably a Hilbert filter in the transmitting section of the SE module;

Fig. 10 shows the frequency response of the first complex output filter according to Fig. 9;

Fig. 11 shows the block diagram of the signal processing at the receiving end in the preamble recognition phase (clear position);

Fig. 12 shows the block diagram of the signal processing at the receiving end in the decryption phase;

Fig. 13 shows an operating and functional sequence diagram for the signal processing at the transmitting end, according to the block diagram in Fig. 6; and

Fig. 14 shows an operating and functional sequence program for the signal processing at the receiving end, according to the block diagrams in

Figures 11 and 12.

In order to simplify understanding, the circuit construction and/or the method of operation of an exemplary embodiment of an SE module according to the invention are/is described in the following text, using a plurality of individual sections:

1. Circuit description of the SE module

The SE module consists essentially of a high-performance, digital signal processor system and the peripheral components required for operation, linked to modern signal processing algorithms. The block diagram shown in Fig. 1 shows the components and assemblies which are important for the digital signal processing. Functions such as the power supply, clock generation, discrete inputs and analog input and output stages are not illustrated, in order to improve the clarity.

The construction of the SE module according to Fig. 1 corresponds to an implemented and working prototype which is still used to some extent for testing and further improvement of the algorithm development. The block diagram illustration itself shows a production design which is being aimed at. The description of this exemplary embodiment is in no way to be understood as the single possible embodiment of the invention. Rather - as the person skilled in the art can see - a large number of modifications and changes are possible in all the sub-areas and assemblies both at the transmitting end and at the receiver end, without departing from the scope of the technical teaching communicated here.

The major signal processing unit is a signal processor 1 in which the ADSP21msp55 processor type, from the Analog Devices Company is used, at least in the prototype design. This signal processor 1 already contains an A/D converter 2 and a D/A converter 3 with a

resolution of, for example, 16 bits and with a sampling rate of 8 kHz. Furthermore, separate RAM regions 2, 3 are integrated for data on the one hand (1k x 16) and program (2k x 24), on the other hand. The internal memory organization corresponds to the Harvard architecture so that one data access is also possible in each command cycle, in addition to the Op-Code-Fetch. All processor operations, without exception, require one cycle. A processing power of 13 MIPS (integer) is thus available.

A mask-programmed variant of this processor (ADSP21msp56) is provided for series production, which will additionally have a 2k x 24 bit-large ROM 6 on the program-memory side.

A further A/D and D/A converter pair 8,9 is required for duplex operation. This is implemented by means of a Type AD28msp02 converter chip 7 which contains the identical converter to the signal processor 1 in a separate housing. The data transmission between the converter chip 7 and the signal processor 1 is carried out via fast serial interfaces.

An EEPROM 10 is provided as the external memory, which accommodates program parts which can be loaded as well as variables which are to be changed rarely, such as the code (see below for further explanation), for example. The memory size in this case is 8k x 8 (production) and 32 k x 8 (prototype), as indicated in Fig. 1.

The status of a voice key, squelch logic of a radio apparatus 11 and a Crypt-ON/OFF switch can be interrogated by the signal processor 1 on discrete input signals (not illustrated).

The operating sequence, further details of which will be described in conjunction with the signal processing, can be briefly described as follows:

After application of the operating voltage, a RESET signal with a duration of several milliseconds is produced first. After this, the signal processor 1 loads its internal program RAM 5 with the content of the external

EEPROM 10 and starts the program. In the case of the prototype of the SE module which is being tested at the moment, the entire program which is required at a specific time must still initially be accommodated in this RAM (2x instructions). In the production configuration of the SE module, which has already been indicated in Fig. 1, 2k instructions are additionally available in the ROM 6.

The external EEPROM 10 can also be addressed as a data memory in order to be able to read and change variable parameters, such as the code, for example.

The program sequence is structured in time by interrupts of the analog interfaces which run freely at their specified conversion rate of 8 kHz and in each case trigger an interrupt after conversion has been carried out.

2. The signal processing

All the functions of the SE module are implemented by digital signal processing.

The principle of the signal processing will be explained first.

Fig. 3 shows the functional block diagram of the transmitting section of the SE module:

A code signal with whose aid the input signal of the microphone, that is to say the voice signal, is encrypted, is generated at the transmitting end in a code signal generator 23. A so-called preamble, which is produced in a preamble generator 24, is transmitted immediately before the encrypted voice signal by operating a PTT key (not illustrated), as can be seen in the three time-related diagram elements in Fig. 2.

The preamble is required for synchronization of a further code signal generator 43 (cf. Fig. 5) and for setting an equalizer 40 at the receiving end.

If it is intended to make it possible to connect into an ongoing conversation, the preamble is transmitted

periodically in a fixed time frame, every 5 seconds in the case of the prototype which is being tested at the moment. The encrypted voice signal is in this case masked out for the duration of the preamble (approximately 200 ms at the moment).

A pilot signal generator 20 supplies a special pilot signal which is additively linked to the encrypted voice signal and which is used at the reception end for synchronization of the sampling clock, as is explained further below in more detail. The front-end unit 22a/22b, which is illustrated in two sub-blocks, carries out the pre-conditioning of the analog input signal and conversion into a digital signal, and the final conditioning of the voice signal encrypted at the transmitting end and matching to the respective transmission device and the transmission channel. Further details are also explained further below.

As can be seen in Fig. 4, the start of an encrypted transmitted signal is characterized by the preamble. For this reason, an analysis of the received signal always takes place at the receiving end whenever the receiver is not in the decryption mode. During this phase the received signal is looped unchanged by the SE module. If the end of a preamble is recognized, the decryption process is started with this recognition, that is to say the code generator 43 at the receiving end is started and the useful signal being received is decrypted ("voice signal" in Fig. 4).

Fig. 5 shows the functional block diagram of the receiving section of the SE module. The received signal is supplied to a functional block 44 whose object is to recognize and analyse the received signal. If a preamble is received, then, using it, the properties of the transmission channel are determined first, and filter coefficients for an equalizer 51 at the receiving end are determined therefrom.

If the end of the preamble is detected, then an

equalizer which is matched to the transmission channel is available at this time. Reference is made to the document DE-C1-41 08 806 (reference [4]) with respect to details of such an initial synchronization and matching of a receiving filter of a digital receiver. At the same time, the code generator 43 at the receiving end is started in order to decrypt the useful signal. The sampling synchronization 55 evaluates the pilot signal superimposed on the useful signal and separates this pilot signal from the useful signal. The decrypted useful signal is subsequently passed on.

Further details are presented in the following detailed description of the transmitting end and of the receiving end.

Fig. 6 shows a detailed block diagram of the signal processing at the transmitting end for the case of decryption. The individual functional blocks are described in more detail in the following sub-sections. All the signal processing functions which are shown by written statements in the sequence diagram in Fig. 13 are implemented with the aid of the one signal processor 1 (cf. Fig. 1). The double lines and double arrows in Fig. 6 are intended to denote analytical signals. Real signals are represented by single lines and arrows.

In principle, it is possible to distinguish between three types of signal processing: Firstly, analog signal processing in the analog front end 22, digital signal processing at the clock rate of 8 kHz, and digital signal processing at the clock rate of 2.667 kHz ($8/3$ kHz). For the illustration in Fig. 6, the corresponding signals are distinguished by the parameter designations t = analog, v = digital, 8 kHz clock and n = digital, 2.667 kHz clock.

A clear text mode is implemented by simple feedback on the digital side of the analog front end 22.

At this point, it should be mentioned that the field of operation of the present prototype of an SE

module according to the invention can be seen in the present-day analog transmission channels.

The analog front-end unit 22 at the receiving end has the object of level matching, sampling of the analog input signal $c(t)$, and conversion into a digital signal $c(v)$.

The A/D converter section of the analog front end 22 (not illustrated in detail) consists of two analog input amplifiers and an A/D converter.

The following specifications apply to the A/D converter section of the analog front end 22 for the tested prototype of the SE module:

Sampling frequency:	8 kHz
Word length:	16 Bit

Decimalization filter

Pass band:	0 to 3.7 kHz
Ripple:	± 0.2 dB
Reverse attenuation:	65 dB

For further details of the construction and operation of the analog front end 22, reference should be made to Ref. [1] and Ref. [2] in the bibliography specified in the Annex, the contents of which references may possibly provide further explanation.

The digitized input signal $c(v)$ acts on a first complex input filter 30 for suppressing the lower sideband. This filter 30 also ensures that the bandwidth of the input signal (digitized voice signal) is limited to a bandwidth which corresponds to that of the transmission channel, that is to say 2.667 kHz in the present exemplary embodiment. The complex first input filter 30 produces, from a real input signal, a complex output signal consisting of a real part and an imaginary part, a phase shift of 90° existing (analytical signal) between the real part and the imaginary part for any desired

frequency. At the same time, spectral elements outside the usable bandwidth of the transmission channel are suppressed. Preferably and in the case of the embodiment of the invention tested, the first complex input filter (in the same way as the complex input filter at the receiving end; cf. further below) is a higher-order Hilbert filter.

The first Hilbert filter 30 at the receiving end is a recursive filter whose transfer function is given by

$$H(z) = \frac{\sum_{i=0}^{16} a_i \cdot z^{-i}}{\sum_{i=0}^{16} b_i \cdot z^{-i}} \quad (1)$$

The structure of this filter is shown in Fig. 7.

The input signal of this Hilbert filter 30 is, as mentioned, the sampled, real received signal $c(v)$. The recursive part of this filter has only real coefficients b_i , so that only real operations are required here, as well. The transverse part has complex coefficients a_i .

The design of this first Hilbert filter 30 is based on the design of an elliptical low-pass filter. The low-pass filter is converted into a Hilbert band-pass filter by transformation in the frequency domain.

The frequency response of the Hilbert filter 30 implemented in the prototype of the invention is shown in Fig. 8.

The band-limited output signal $d(v)$ of the first complex input filter (Hilbert filter) acts on a functional block which is designated as sampling rate reduction 31 and in which the sampling clock is reduced by a specific, preferably integer factor, in the present exemplary embodiment by the factor 3, to 2.667 kHz. Suitable dimensioning of the first Hilbert filter 30 on the input side ensures that no aliasing effects occur.

The combination of the Hilbert filter 30 and the sampling reduction 31 leads to a randomly selected frequency band with a 2.667 kHz bandwidth containing all the useful information.

In principle, only every third output value of the input-side signal $c(v)$ of the Hilbert filter 30 is used for sampling rate reduction. In practice, this is implemented by the transverse part of the Hilbert filter 30 being operated at 8/3 kHz. This means that the filter output values are calculated and further-processed only with every third clock pulse of the 8 kHz sampling clock.

The pilot signal generator 20 is used for producing a pilot signal $q(n)$ which is used at the receiving end for clock slaving. The pilot signal is produced by the phase modulation, which is described further below, of the pilot signal.

The (pseudo-)random-number generator 34 (cf. Fig. 6), as part of the code signal generator 23, has the object of producing equally distributed numbers in the range from, for example, 1 to 64. These numbers are used for the purpose of selecting random values from a field of 64 complex values (cf. "data set" block in Fig. 6). Two code signals $z_s(n)$, $z_p(n)$ are produced from the selected values, one ($z_s(n)$) of which code signals is used for phase modulation of the useful signal and the second ($z_p(n)$) is used for producing the pilot signal $q(n)$.

The random-number generator 34 which is implemented in the present embodiment of the invention is based on the linear congruence method. The random values $r(n)$ are calculated in accordance with the rule

$$r(n) = (a \cdot r(n-1) + c) \bmod m \quad n = 1, 2, \dots \quad (2)$$

The start value $r(0)$ is in general unimportant since all m possible values are produced before the random sequence is repeated if the constant values a and c are suitably

selected. The random numbers generated are distributed uniformly in the range from 0 to $(m-1)$.

In the case of the embodiment tested, $m = 2^{32}$ was selected. This allows a long sequence to be produced. In addition, the Modulo function of the equation (2) can then be implemented by the signal processor 1 with very little complexity.

The constants were selected to be $a = 1664525$ and $c = 32767$ in accordance with Knuth's rule (cf. Ref.[6]).

In order to obtain uniformly distributed random numbers between 1 and 64, it is sufficient to consider 6 bits of the respective random value $r(n)$ and to use them further as a random number. In the case of the present embodiment, 6 bits are used for generation of random numbers for the "scrambling" (the phase modulation) of the useful signal $x(n)$ and 6 bits for generation of random numbers for the "scrambling" (the phase modulation) of the pilot tone $p(n)$. Thus, the random-number generator 34 supplies two random numbers $r_s(n)$ and $r_p(n)$ in each case in each clock cycle.

After each transmission of a preamble, the random-number generator 34 is reinitialized with a defined start value $x(0)$.

The control values for the phase modulators 32 and 33 are represented by a data set of 64 complex values. The random-number generator 34 selects values from this set and thus produces a random signal for phase modulation.

The 64 complex values

$$a_i = e^{j2\pi i/64} \quad i = 1, 2, \dots, 64 \quad (3)$$

are used as the data set. The control or input values $z_s(n)$ and $z_p(n)$ all have the amplitude "1", but are in different phases. The random-number-controlled phase modulators 32, 33 are explained in more detail in the following text.

Two phase modulator units 32 and 33 are required in the transmission section of the SE module (Fig. 6). One phase modulator 33 is required for the encryption of the useful signal $x(n)$ by means of a code signal $z_s(n)$ supplied by the random-number generator 34. The other phase modulator 32 is used for generating the pilot signal $q(n)$ from the pilot tone $p(n)$, which is supplied by the pilot-tone generator, with the aid of the other code signal $z_p(n)$. Since the code signals $z_s(n), z_p(n)$ are random sequences of complex values having the same amplitude but different phases, each phase modulator 32, 33 carries out a complex multiplication of the respective input signal value by the respective code signal value.

If, as Fig. 6 shows, the signal values of the analytical filter output signal are designated by $x(n)$ and the signal values of the associated code signal by $z_s(n)$, then, for the signal values of the phase-modulated useful signal:

$$y(n) = x(n) \cdot z_s(n) \quad (4)$$

The phase-modulated useful signal $y(n)$ has a character like a noise signal. The information contained in the useful signal is completely distributed over a frequency band with a width of 2.667 kHz.

At this point it should be mentioned that the phase modulation according to the invention has a certain similarity to a 64-stage PSK modulation as is used in digital transmission technology. However, the purpose in the present example is quite different:

In the case of digital data transmission using PSK modulation, the phase of a carrier signal is keyed at the sampling clock rate (Phase Shift Keying). The phase of the carrier signal thus contains the digital information to be transmitted. At the receiving end, the phase of the carrier is determined at defined sampling times. A discriminator assigns the corresponding digital

information to each determined phase and thus obtains the transmitted information.

On the other hand, in the case of the phase modulation proposed here according to the invention, the signal to be modulated carries the information to be transmitted, rather than the modulation signal. This information is predetermined by its quasi-continuous signal profile. The phase modulation is used only for the purpose of changing the signal to be transmitted such that it is no longer possible to deduce the original signal profile. A voice signal thus becomes completely incomprehensible. The useful information is encrypted by the phase modulation.

At the receiving end, the useful information can be recovered by the inverse operation to the equation (4)

$$x(n) = \frac{\hat{y}(n)}{z_s(n)} \quad (5)$$

Complete recovery is possible only when two conditions are satisfied. Firstly, the received signal $y(n)$ must correspond with the (phase-modulated) transmitted signal $y(n)$. Secondly, the modulation signal, that is to say the code signal $z_s(n)$, must be known at the receiving end.

The first requirement is dependent on the equalization of the transmission channel at the receiving end. The second requirement is dependent on the knowledge of the code signal and exact synchronization at the receiving end.

While the number of values of the code signal $z_s(n)$ is defined by the number of steps in the modulation (64 in this case), the number of possible values for $x(n)$ and $y(n)$ is determined by the word length in the signal processing.

If the signal values of the generated pilot tone are designated by $p(n)$ and the signal values of the associated code signal by $z_p(n)$, then the signal values

of the pilot signal are given by the relationship

$$q(n) = p(n) \cdot z_p(n) \quad (6)$$

Thus, because of the properties of the selected random-number generator 34, the pilot signal $q(n)$ thus generated is white noise.

In order to be able to transmit the analytical signal generated at the clock frequency of 2.667 kHz, the transmitted signal must be matched to the transmission channel. Since, in the example illustrated, the sampling frequency predetermined by the analog front end 22 is 8 kHz, a sampling rate increase to 8kHz must be carried out first.

The increase in the sampling rate by the factor of 3, that is to say from 2.667 kHz to 8 kHz, is achieved by insertion of two signal values in each case, having the value 0, between two existing signal values, that is to say

$$d_s(v) = \dots, w(n-1), 0, 0, w(n), 0, 0, w(n+1), \dots \quad (7)$$

The sampling rate increase is carried out in conjunction with a first complex output filter 35 for matching the analytical transmitted signal to the transmission channel. The real part of the analytical output signal of this complex output filter 35 is supplied to the analog front end 22.

The first complex output filter 35 initially produces from a complex input signal $d_s(v)$ an analytical signal whose real part and imaginary part are phase-shifted through 90° for any given frequency, and, from this, a real output signal $c_s(v)$. At the same time, spectral elements outside the useable bandwidth of the transmission channel are suppressed.

The first complex filter 35 on the output side is preferably a (second) Hilbert filter, that is to say a

recursive filter, whose structure is shown in Fig. 9.

The input signal $d_s(v)$ of this second Hilbert filter 35 is, as mentioned, an analytical signal; the output signal $c_s(v)$, on the other hand, is a real signal.

The design of the filter is based on the design of an elliptical low-pass filter. The low-pass filter is subsequently converted into a Hilbert band-pass filter by transformation in the frequency domain.

The frequency response of the (second) Hilbert filter 35 on the output side at the transmitting end is shown in Fig. 10.

The conversion of the digital output signal $c_s(v)$ of the second Hilbert filter 35 into an analog output signal is carried out in the output section of the analog front end 22 (reference note 22b in Fig. 3). This conversion also includes local matching.

In the implementation, the D/A converter part 3 (Fig. 1) of the analog front end 22 (without any detailed illustration) consists of a D/A converter, an analog smoothing filter, a programmable amplifier and a differential amplifier.

The following specifications apply to the output of the analog front end 22 in the illustrated exemplary embodiment of the invention:

Clock frequency:	8 Khz
Word length:	16 bits
Gain:	Adjustable in the range from -15 dB to + 6 dB
Interpolation filter	
Frequency response:	0 to 3.7 kHz
Ripple:	± 0.2 dB
Reverse attenuation:	65 dB

Once again, reference should be made to Ref. [1] and Ref. [2] for more detailed information on the transmitting-end output at the analog front end 22.

The preamble generator 24 is used for generating a preamble at the start of the transmission via radio channels or telephone channels. In order to make it possible to connect to an ongoing transmission at the receiving end, the generation of a preamble is initiated at fixed time intervals.

The preamble which is used consists of two successive signal sections. The first signal section is a so-called CPFSK signal (Continuous Phase Frequency Shift Keying). The second section is a noise-like signal. The first part is used in the receiver for the detection of the preamble and for synchronization of the receiver. The second signal part is used for equalization of the transmission channel.

The CPFSK signal is generated by the CPFSK modulation of a special data frequency. The length of this sequence is, for example, 240 bits. The transmission rate is 1.778 kbit/s. The construction of the data sequence is selected such that very reliable detection of the preamble is possible using a special method at the receiving end. Once again, reference is made to the document DE-C1 41 08 806 (Ref. [4]) and to Ref. [5] for further details.

Overall, the duration of the preamble in this example is approximately 230 ms.

Two different operating modes of the SE module can be distinguished at the receiving end. One of these is the phase of the preamble recognition during which the SE module is in the clear position, and the other is the decryption phase. In the same way as the transmitting end, three types of signal processing can be distinguished, namely analog signal processing, digital signal processing at the 8 kHz clock rate and digital signal processing at the clock rate of 2.667 kHz. The calculation of the equalizer coefficients runs in the background, without being linked to a specific sampling clock.

After the apparatus has been switched on, the SE module is always in the preamble recognition phase. Fig. 11 shows the functional block diagram of the signal processing. In this phase, the received signal passes only through the analog front end 52 with its filter. The received signal remains essentially uninfluenced by the SE module.

The sampled received signal (8 kHz sampling frequency, 16 bit word length) is supplied after filtering to a second complex input filter 14 at the receiving end, especially to a third Hilbert filter (band-pass filter) and to a sampling rate reduction 43 to 2.667 kHz to the preamble recognition block 55. At the same time, the sample values of the received signal are buffer-stored in the buffer 41. The preamble recognition block 55 detects the reception of the preamble automatically and very reliably. References can be found in Ref. [4] (DE-C1-41 08 806) and Ref. [5].

The operation and structure of the second complex input filter 40 correspond essentially to the first complex input filter 30 at the transmission end, described above.

The preamble recognition has two functions: firstly the detection of the reception of the preamble and the changeover to decryption. Secondly, the preamble supplies an exact time reference. This is necessary for the initialization and synchronization of the decryption process.

Thus, in particular, the initialization of a random-number generator 34 at the receiver end and of a pilot-signal generator 50 takes place with the recognition of the preamble. In addition, a process for determining equalizer coefficients is initiated. The calculated coefficient set is used to set an equalizer 51 which is required for the decryption mode.

The second section of the preamble, that is to say the noise signal, is evaluated to determine the

equalizer coefficients. This means waiting until a specific part of this section is in the buffer 41. The pulse response and the coefficient set for the equalizer filter 51 are then calculated with the aid of an FFT (Fast Fourier Transformation) and a nominal spectrum which is present in the receiver and is stored in the program RAM 5 (Fig. 1).

After recognition of the preamble, the SE module is in the decryption mode. Fig. 12 shows the signal processing in this phase. The sequence diagram for the functional sequence steps of the signal processing at the receiving end are shown in Fig. 14.

The received signal is converted by the analog front end 52 into a digital signal with, for example, an 8 kHz sampling frequency and a 16 bit word length. This signal passes through the equalizer 51, whose object is equalization of the transmission channel, as is explained in more detail further below. After filtering via the second complex input filter 40 (especially a third Hilbert filter; band-pass filter; likewise described in more detail further below) and a sampling rate reduction 43 by the factor 3, an analytical signal is present with the sampling frequency 2.667 kHz. This signal $s(n)$ consists of the encrypted useful signal and the superimposed pilot signal. As described above, the pilot signal is a phase-modulated signal. The pilot signal is evaluated and separated from the useful signal in the clock synchronization block 45. The decryption of the useful signal is carried out subsequent to this, by a phase demodulator (descrambler) 59.

Once a sample rate increase 61 to 8 kHz and subsequent filtering using a second complex output filter 62, especially a fourth Hilbert filter (band-pass filter) has been carried out, the conversion into an analog signal in the receiver-end analog front end 52 takes place. This signal is the decrypted audio signal.

The operation and the construction of the second

complex output filter 62 correspond essentially to those of the first complex output filter 35.

The evaluation of the pilot signal in the clock synchronization block 55 additionally supplies a controlled variable for regulating out fluctuations in the sampling clock (clock correction). The regulation of the sampling clock is necessary because of the stringent requirements for synchronicity during the decryption. Fluctuations in the sampling clock are caused by scatter between equipment and drifts of the crystal oscillators used.

In order to evaluate the pilot signal, the received signal $\hat{s}(n)$ at a reduced sampling rate passes through a phase demodulator (descrambler) 58. The output signal $\hat{q}(n)$ of this phase modulator 58 consists of a carrier signal element and a superimposed signal element like a noise signal, which is produced from the useful signal. The carrier signal is converted into the baseband signal using the signal generated by the pilot-tone generator 50. After an averager 56, an analytical baseband signal is available whose real part is a measure of the level of the pilot signal and whose imaginary part is used as a controlled variable for regulating the sampling clock.

Using the determined level of the pilot signal, the pilot-signal generator 50 and a phase demodulator (scrambler) 57, a pilot signal $q(n)$ is generated at the receiving end and is subtracted from the received signal $\hat{s}(n)$. In the ideal case, the generated pilot signal $\hat{q}(n)$ corresponds exactly to the received pilot signal, so that the useful signal is completely separated from the pilot signal by the subtraction. If the equalization is optimal, then the signal $\hat{y}(n)$ obtained from the subtraction process corresponds, except for any superimposed noise signal, with the signal $y(n)$ at the output of the phase modulator 33 at the transmitting end (cf. Fig. 6).

The phase modulator 57 and the two phase demodulators 58, 59 are controlled by two

(pseudo-)random-number generators 54. One random-number generator controls the phase modulator 57 and the phase demodulator 58 of the clock synchronization block 55, the other controls the phase demodulator 59 for decryption of the useful signal $y(n)$. The random-number generators correspond to those at the transmitting end; they are synchronized to the received signal, in the same way as the pilot-signal generator 50, by the recognition of a preamble.

The objects and the implementation of the individual functional blocks in Fig. 12 are described in detail in the following text.

The input section of the analog front end 52 has the object of level matching, sampling the analog received signal, and conversion into a digital signal.

Once again, the AD28msp02 chip from the Analog Devices Company is used as the analog front end 52 in the prototype implementation (cf. Ref.[3]). This chip corresponds exactly to the analog front end used in the ADSP-21msp55 signal processor.

Once again, the analog front end 52 consists of two analog input amplifiers, a 20 dB preamplifier which can be connected and an A/D converter.

The following specifications apply to the A/D converter section of the analog front end 52:

Sampling frequency:	8 kHz
Word length:	16 Bit
Decimalization filter	
Pass band:	0 to 3.7 kHz
Ripple:	± 0.2 dB
Reverse attenuation:	65 dB

The equalizer 51 is used for equalization of the frequency response of the transmission channel in the region of the transmission bandwidth from, for example,

300 Hz to 3 kHz. The transmission channel contains all the assemblies from the first complex output filter 35 of the transmission section to the second complex input filter 40 of the receiving section (both inclusive).

The equalizer 51 is implemented by a transverse digital filter having 128 stages. The transfer function is:

$$E(z) = \sum_{i=0}^{127} e_i \cdot z^{-i} \quad (11)$$

The coefficients e_i are determined during the reception of one preamble.

The second complex input filter 40 (Hilbert filter) is used for suppressing the lower sideband of the input signal and for limiting the bandwidth of the input signal (received voice signal) to a bandwidth of approximately 2.66 kHz.

The second complex input filter 40 (Hilbert filter) is a recursive filter whose structure corresponds to that of the input-side first complex filter 30 so that, to this extent, reference can be made to Fig. 7.

The input signal of the second complex input filter 40 is the real output signal $c(v)$ of the equalizer 51.

The design of this filter is based on the design of an elliptical low-pass filter. The low-pass filter was converted into a Hilbert band-pass filter by transformation in the frequency domain.

A sampling rate reduction 43, in order to reduce the sampling rate in the illustrated example by the factor "3" to 2.667 kHz, is also carried out in the receiving section, in an analogous manner to the transmitting section. Suitable dimensioning of the second complex input filter 40 ensures that no aliasing effects occur.

The combination of a complex input filter 40 and sampling rate reduction 43 leads to any selected frequency band having a 2.667 kHz bandwidth containing all the useful information.

In practice, the processing of each third output value of the second complex input filter 40 is implemented in that the transverse part of this filter is operated at 8/3 kHz. This means the filter output values are calculated and further-processed only in each third clock cycle of the 8 kHz sampling clock.

The pilot-tone generator 50 supplies an identical signal to that of the pilot-signal generator 37 at the transmitting end. This signal is required in the clock synchronization block 55 for conversion of the received and demodulated pilot signal $\hat{q}(n)$ into the baseband signal, and for the receiving-end generation of a phase-modulated pilot signal $p(n)$.

As already mentioned above, the averager 56 is used for averaging the analytical signal $\hat{q}(n)$ transformed into the baseband, so that the level of the received pilot tone is produced as the real part and a controlled variable for sampling clock slaving (clock correction) is produced as the imaginary part.

The averaging is implemented such that, after every 128 sampling clock cycles, the mean is formed over the last 128 input signal values $\hat{q}(n)$, transformed into the baseband signal.

The random-number generator 54 has the object of producing uniformly distributed numbers in the range from 1 to 64, entirely analogously to the random-number generator 34 at the transmitting end. These numbers are once again used in order to select random values from a field of 64 complex values. Once again, two code signals $z_p(n)$ and $z_s(n)$ are produced from the selected values, of which one ($z_s(n)$) is used for phase demodulation, that is to say for decryption of the useful signal $\hat{y}(n)$, and the second ($z_p(n)$) is used in the clock synchronization block

55 on the one hand for decryption of the received pilot signal and on the other hand for generation of the receiving-end pilot signal. Because of the clock synchronization, the code signals are, of course, identical to the code signals $z_p(n)$ and $z_s(n)$ at the transmitting end.

The implementation of the random-number generator 54 is otherwise identical to the implementation in the transmitting section, so that reference can be made to the above designs.

The random numbers supplied to the phase modulator 57 and to the phase demodulators 58 and 59 consist of a set of 64 complex values, from which discrete values are selected by the random-number generator 54. In an analogous manner to the transmitting end, the same 64 complex values

$$a_i = e^{j2\pi i/64} \quad i = 1, 2, \dots, 64 \quad (8)$$

are used as the data set.

The two already mentioned phase demodulators 58, 59 are required in the receiving section of the SE module. One phase demodulator 59 is used for decryption of the useful signal $\hat{y}(n)$ by the one code signal $z_s(n)$. The other phase demodulator 58 is used for recovery of the pilot tone from the received pilot signal. As already mentioned, these code signals must be identical to the code signals at the transmitting end.

If the signal values of the analytical input signal after the sampling reduction 60 are designated by $\hat{s}(n)$ and the signal values of the code signal of the pilot tone are designated by $z_p(n)$, then, for the signal values at the output of the phase demodulator 58 in the clock synchronization block 55:

$$\hat{q}(n) = \frac{\hat{s}(n)}{z_p(n)} \quad (10)$$

If the encrypted useful signal is designated by $\hat{y}(n)$ and the code signal for the encryption is designated by $z_s(n)$, then, for the decrypted signal at the output of the phase demodulator 59:

$$\hat{x}(n) = \frac{\hat{y}(n)}{z_s(n)} \quad (11)$$

The phase demodulator 57 is used for generating the pilot signal from the pilot tone supplied by the pilot-tone generator 50.

If the signal values of the generated pilot tone are designated by $p(n)$, then the signal values of the phase-modulated pilot tone result from the relationship:

$$q(n) = p(n) \cdot z_p(n) \quad (12)$$

In order to be able to convert the digital analytical signal $\hat{x}(n)$ which is generated at a clock frequency of 2.667 kHz into an analog signal, it is first necessary to carry out a sampling rate increase to 8 kHz.

The increase in the sampling rate by the factor 3 - that is to say from 2.667 kHz to 8 kHz in the illustrated example - is carried out by inserting two signal values having the value "0" in each case between two signal values, corresponding to the following relationship:

$$\hat{d}_s(v) = \dots, \hat{x}(n-1), 0, 0, \hat{x}(n), 0, 0, \hat{x}(n+1), \dots \quad (13)$$

A further (second) complex output filter 62, preferably a (fourth) Hilbert filter, is used for converting the analytical output signal into a real output signal. This filter is used to limit the bandwidth of the output signal (voice signal) to approximately 2.667 kHz.

The second complex output filter 62 is once again a recursive filter whose structure corresponds to that of the first complex output filter 35 at the transmitting end and is shown in Fig. 9.

The input signal of the second complex output filter 62 (fourth Hilbert filter) is once again an analytical signal. The output signal is a real signal.

In the case of the exemplary embodiment of the invention tested, the design of the filter is based on the design of an elliptical low-pass filter. The low-pass filter is converted into a Hilbert band-pass filter by transformation in the frequency domain.

The analog front end 52 on the output side has the object of converting the digital output signal into an analog output signal (audio signal). This also includes the level matching.

The D/A converter section, which is not illustrated in detail, of the analog front end 52 (output) consists of a D/A converter, an analog smoothing filter, a programmable amplifier and a differential amplifier.

The following specifications apply to the output of the analog front end 52:

Clock frequency:	8 kHz
Word length:	16 Bit
Gain:	Adjustable in the range from -15 dB to +6 dB
Interpolation filter	
Frequency response:	0 to 3.7 kHz
Ripple:	± 0.2 dB
Reverse attenuation:	65 dB

The essence of the invention is in no way limited to the described embodiment of an SE module. Extension options, primarily with respect to the security of the encryption, can be identified by the person skilled in the art on the basis of the invention. In the case of the described exemplary embodiment, only a simple (pseudo-)random-number generator is used for generating the code signals. The use of separate, different generators is a possibility for further improvement of the encryption security.

In addition, in the case of the described exemplary embodiment, it has also been assumed that the random-number generator 54 used starts at the same starting point on every resynchronization. The security of the encryption can be increased if the starting point is changed on every resynchronization. This can be achieved by the starting point of the random-number generator 54 being transmitted in the preamble.

BIBLIOGRAPHY

- [1] Analog Devices: ADSP-2100 Family User's manual. Prentice Hall, 1993.
- [2] Analog Devices: ADSP-21msp50/55/56 Datasheet, Mixed-Signal-Processor.
- [3] Analog Devices: AD28msp02 Datasheet, Voiceband Signal Port.
- [4] DE-C1 41 08 806 $\hat{=}$ US-5,267,264
- [5] E. Schlenker: Ein Verfahren zur Bestimmung des signalangepaßten Empfangsfilters und der Anfangssynchronisation eines digitalen Empfängers. [A method for determining the signal-matched receiving filter and the initial synchronization of a digital receiver]. Dissertation, Stuttgart University, Institut für Netzwerk- und Systemtheorie [Network and System Theory Institute], 1993.
- [6] D.E. Knuth: The Art of Computer Programming: Volume 2/Seminumerical Algorithms, Second Edition, Reading, MA: Addison-Wesley Publishing Company, 1969.



PATENT CLAIMS

1. Method for speech encryption and decryption in voice transmission, characterized in that at the transmitting end

- the digitized voice signal $c(v)$ is converted by means of a first complex input filter (30) having a bandwidth which corresponds to the bandwidth of the transmission channel into a complex signal $x(n)$ which is phase-modulated by means of a code signal $(z_s(n))$ which is controlled by pseudo-random numbers,
- the phase-modulated voice signal $(y(n))$ is additively combined with a pilot signal $(q(n))$, which is likewise phase-modulated in a pseudo-random distribution, to form an encrypted useful signal $(s(n))$ which is to be transmitted and
- the useful signal $(s(n))$ passes through a first complex output filter (35) in a sequential manner together with a preamble, which is used for synchronization and useful signal equalization at the receiver end, as a complex signal $(w(n))$, which output filter (35) produces a real output signal $(c_s(v))$ which, after digital/analog conversion, is passed to a transmitted signal conditioner, and in that

at the receiving end

- the digitized received signal $(c(v))$ is converted into a complex signal $(s(n))$ by means of a second complex input filter (40) having a bandwidth which corresponds to the bandwidth of the transmission channel,
- from this complex signal $(s(n))$ and during a preamble recognition phase, on the one hand clock synchronization for a pilot signal $(q(n))$, which is produced at the receiver end and is phase-modulated in a pseudo-random sequence initialized by the



preamble, is forced and, on the other hand, equalizer coefficients are calculated for an equalizer (51) at the receiver end and the phase of the useful signal decryption is thus initialized,

- the encrypted useful signal ($s(n)$) is separated from its phase-modulated pilot signal, which is superimposed at the transmitter end, by linking with the synchronized pilot signal ($q(n)$) which is produced at the receiver end, and

- the phase-modulated, encrypted digital voice signal ($y(n)$) which is thus obtained is decrypted by inverse phase modulation by means of the code signal ($z_c(n)$) which is produced at the receiver end and is clock-controlled by means of the preamble and, as a complex signal ($x(n)$) passes through a second complex output filter (62) which produces a real output signal ($c_s(v)$) which, after digital/analog conversion, is passed to a received signal conditioner.

2. Method according to Claim 1, characterized in that higher-order Hilbert filters are used as the complex input and output filters (30, 40 and 35, 62 respectively).

3. Method according to Claim 1 or 2, characterized in that, both at the transmitting and at the receiving end, a sampling rate reduction is carried out in conjunction with a band-limiting complex input filtering and a corresponding sampling rate increase is carried out before the complex output filtering, which is matched to the sampling rate increase.

4. Method according to Claim 3, characterized in that the sampling rate reduction is carried out in an integer ratio, especially in the ratio 1:3, and the sampling rate increase is accordingly likewise carried out in an integer ratio, especially in the ratio 3:1, and in that higher-order recursive filters are used as the complex filters (30, 35, 40, 62).

5. Method according to one of the preceding claims,



characterized in that the preamble is transmitted periodically in a fixed time frame, and the encrypted voice signal is masked out for the duration of the preamble.

6. Method according to Claim 5, characterized in that the fixed time frame lasts for a plurality of seconds, especially 3 to 10 s, and the duration of the preamble is several 10 ms, especially approximately 200 ms.

7. Method according to Claim 6, characterized in that the properties of the transmission channel are tested at the receiver end during the reception of the preamble, and the filter coefficients for the receiving-end equalizer (51) are determined from this.

8. Method according to Claim 7, characterized in that the end of each transmitted preamble is detected at the receiver end for resynchronization, and a pseudo-random number generator (54) for a code generator is started, using the obtained signal, in order to decrypt the useful signal.

9. Method according to one of Claims 1 to 7, characterized in that the random-number-controlled phase modulation of the digitized voice signal and of the pilot signal is carried out by different random-number generators.

10. Method according to one of the preceding claims, characterized in that, in order to increase the encryption security, the starting point for the random number generator or generators (54) at the receiver end within the preamble can be set variably.

11. Device for speech encryption and decryption in apparatuses for voice transmission which are equipped with a front-end unit (22, 52) for digitizing a voice signal and matching a transmitted signal to a predetermined transmission channel on the one hand and/or for digitizing a received signal and for matching of the conditioned received signal to a voice reproduction device on the other hand, characterized in that,



at the transmitting end

- a code generator (23) which is controlled by a (pseudo)-random-number generator (34) acts on a digital phase modulator (33) which phase-modulates the digitized voice signal,
- the phase-modulated voice signal ($y(n)$) is combined with a pilot signal ($q(n)$), which is supplied by a pilot-signal generator (20) and is likewise phase-modulated in a random distribution, to form a useful signal ($s(n)$),
- a preamble generator (24) produces a preamble ($v(n)$) which is used for synchronization at the receiver end and for useful-signal equalization and is emitted sequentially and together with the useful signal, via a changeover switch (25) which can be operated in a defined clock sequence, to the front-end unit (22) for transmitted signal conditioning, and in that

at the receiving end

- there is a digital equalizing filter (51) for equalization of the transmission channel of the digitized received signal, whose equalizer coefficients are calculated and set during the reception of the preamble,
- a device (44) is provided for detection of the preamble within the received useful signal, which device initiates, as a function of a defined section of the preamble, the calculation of the filter coefficients for the equalizer filter (51) in a higher-level computation unit and thus initializes the decryption of the useful signal by activating a clock synchronization device (55) which, on the one hand, supplies from the received, demodulated pilot signal a control signal for sampling clock correction, by complex multiplication (63) by a pilot tone (50) which is generated at the receiving end and, on the other hand, under the control of a random-number



generator (54) which is likewise initialized with the clock synchronization, supplies, from the pilot tone which is supplied by the pilot-tone generator (50) at the receiving end and via a modulator (57), a phase-modulated pilot signal ($q(n)$) which is subtractively linked with the equalized useful signal ($s(n)$) in order to separate the transmitted pilot signal and is thus converted, as a phase-modulated voice signal, in a phase demodulator (59) and controlled by the synchronized random-number generator (54) at the receiving end, into the unmodulated, digital voice signal which is passed to the front-end unit (52) for conversion into an audio signal.

12. Device according to Claim 11, characterized by a (first) device (31) at the transmitting end for sampling rate reduction, which device (31) passes the digitized voice signal supplied by the front-end unit (52) at the transmitting end to the phase-modulation device, after band limiting via a first complex input filter (30) on the input side, at a sampling rate reduced by a fixed factor.

13. Device according to Claim 11 or 12, characterized by a (first) device (36) at the transmitting end for sampling rate increasing, which device (36) increases the speech-encrypted transmitted signal ($w(n)$), which is composed of the useful signal ($s(n)$) and the preamble ($v(n)$) by signal values which are determined by a fixed factor and passes said signal via a first complex output filter (35) to the front-end unit (22) for transmitted signal conditioning.

14. Device according to Claim 12 or 13, characterized by a (second) device (60) at the receiving end for sampling rate reduction, which device (60) passes the digitized received signal, which is supplied by the front-end unit (52) at the receiving end, on to the phase modulation device (55, 59), after equalization and band



limiting, via a second complex input filter (40) at a sampling rate which is reduced by a fixed factor.

15. Device according to Claim 14, characterized by a (second) device (61) at the receiving end for increasing the sampling rate, which device (61) increases the modulated received signal $(x(n))$ by signal values determined by a fixed factor and passes them on via a second complex output filter (62) to the front-end unit (52) at the receiving end, for audio signal conditioning.

16. Device according to Claims 12 and 13 as well as Claims 14 and 15, characterized in that the factor for the sampling rate reduction and the factor for the sampling rate increase are selected to be equal and integer.

17. Device according to Claim 16, characterized in that both factors are selected to be "3".

18. Device according to one of the preceding Claims 11 to 17, characterized in that the random-number generator (34) at the transmitting end and the random-number generator (54) at the receiving end supply random values $(r(n))$ in accordance with the linear congruence method and corresponding to the rule

$$r(n) = (a \cdot r(n-1) + c) \bmod m$$

where $n = 1, 2, \dots$, as an integer, a and c designating integer constants and m designating a selectable number.

19. Device according to Claim 18, characterized in that the integer constants are defined to be $a = 1664525$ and $c = 32767$, and m is selected to be $m = 2^{32}$.

20. Device according to Claim 11, characterized in that the control signal for clock correction and a controlled variable for the level of the pilot signal produced at the receiving end from averaging (56) of the demodulated received pilot signal are obtained over a fixed number of sample values.

21. Device according to one of the preceding Claims



11 to 20, characterized in that the different code signals are in each case used for the statistical phase modulation of the voice signal at the transmitting end and for the demodulation (59) of the received signal after separation of the pilot signal, as well as for the transmitting-end phase modulation of the pilot tone and the receiving-end demodulation of the pilot signal.

22. Device according to one of the preceding Claims 11 to 21, characterized in that Hilbert filters (30, 35, 40, 62) operating as higher-order recursive filters are used as complex filters.