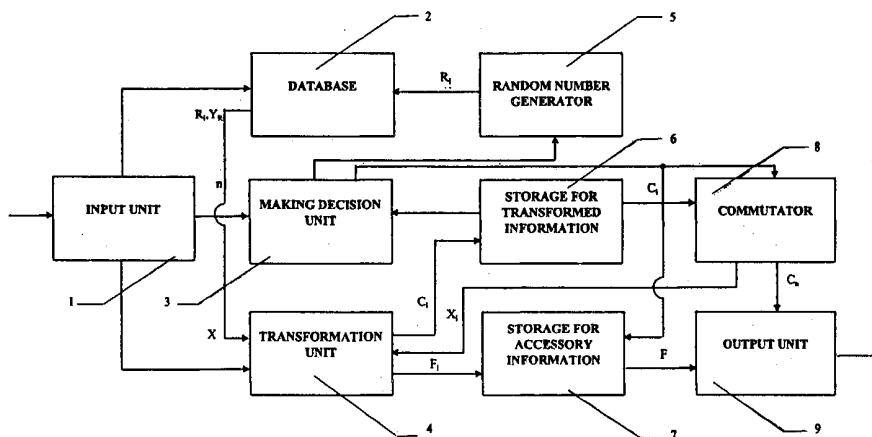




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁷ : H04L 9/06</p>	<p>A1</p>	<p>(11) International Publication Number: WO 00/65767 (43) International Publication Date: 2 November 2000 (02.11.00)</p>
<p>(21) International Application Number: PCT/BY99/00005 (22) International Filing Date: 27 April 1999 (27.04.99) (71)(72) Applicant and Inventor: MISCHENKO, Valentin Alexandrovich [BY/BY]; 28-210, Nekrosova Str., Minsk, 220040 (BY). (72) Inventors; and (75) Inventors/Applicants (for US only): ZAKHARAU, Uladzimir Uladzimirovich [BY/BY]; 1-2-22, 50 Let Pobedy Str., Minsk, 220056 (BY). VILANSKI, Yuri V. [BY/BY]; 10-44, Kuleshova Str., Minsk 220026 (BY). VERZHBALOVICH, Dzmitry I. [BY/BY]; Mvizrū Pvo, Minsk 220057 (BY). (74) Agent: VINOGRADOV, Sergei Gennadievich; P.O. Box 261, Minsk, 220006 (BY).</p>		<p>(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>With international search report.</i></p>

(54) Title: METHOD FOR ENCRYPTING INFORMATION AND DEVICE FOR REALIZATION OF THE METHOD



(57) Abstract

The invention relates to means for protecting information from an unauthorised access by electronic means. In order to transform the initial information the device has the transformation unit (4), the making decision unit (3), the storage of the recovered communication (6), the commutator (8), and for storing the accessory information the device has the storage of the accessory information (7). For encoding and transferring information the addressee is beforehand provided with a key to the received communications with information on regularities corresponding to the values of the communication transmitted to him, with specific values of the initial information for the whole set of symbols of the said kind of an information. In this case the addressee is beforehand provided with a set of transformation functions, $Y_1, Y_2, \dots, Y_N = Y_i(X)$, where $X = \{x_1, x_2, \dots, x_m\}$ is a plurality of specific symbols of the transformed information. In the course of processing the encrypted information the input of the making decision unit (3) enters the information on the number (n) of transformation cycles of the initial communication. Before the beginning of the current transformation cycle, the making decision unit (3) transmits a control signal to the generator of random numbers (5), which generates a random number (R_i), transmits it to the data base (2) and through the latter to the transformation unit.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

5 METHOD FOR ENCRYPTING INFORMATION AND DEVICE FOR REALIZATION OF THE METHOD

The invention relates to means for protecting information from an unauthorized access, and may be used in crypto-systems for encoding,
10 transferring and decoding communications, and in other systems for protection of information.

The prior art discloses engineering solutions providing protection of transmitted information by means of a special equipment or encoding software, for example by using scrambler for protection of telephone conversations [1] pp. 35-
15 37, Fig. 22. The scrambler operates on the principle on inversion of an audio signal. As a result of an inversion a usual speech turns to a senseless gang of sounds, but the initial signal is accepted by the user without any distortion. The telephone set is equipped with the block for voice modification controlled by the encoder. The encoder stores 13122 user's codes providing 52488 digital
20 combinations. The read-only memory of the set stores the resident software, which codes and decodes the transmitted information in several variants and controls the work of the whole set.

However this prior art solution has problems in providing a fair degree of secrecy, since for disclosing the confidential codes it is enough to execute a
25 limited number of mathematical operations that are fast and effectively executed by the modern high-speed electronic engineering.

The main characteristic of a crypto-system is the degree of secrecy. The task of a cryptographer is to provide the utmost secrecy and authenticity of the transferred information. Alternatively, a crypto-analyst "forces open", or "breaks",
30 the crypto-system designed by a cryptographer. The crypto-analyst tries to decipher the set of encoded symbols and to deliver the encrypted communication as the plaintext.

Prior art discloses technical solutions for protecting the transferred information by using a specific device and/or encoding software. Known codes
35 are based on two simple methods: substitution and interchange. Interchange uses

simple mixing of plain-text symbols, the key of an interchange encryptor defines the specific type of mixing. The frequency distribution of individual symbols in the encoded text is identical to that of the plaintext. For substitution, each symbol of the plaintext is replaced by another symbol of the same alphabet, and the specific
5 type of substitution is determined by the secret key.

For example, the algorithm in the Data Encryption Standard (DES) [2], p. 33-34 uses the both methods. The algorithm comprises plaintext, unencrypted text and the key as binary sequences having the length 64, 64 and 56 bits, respectively. When DES is used in an electronic book or table mode, the 64-bit
10 blocks of the plaintext are encoded independently by using one key. The algorithm of DES includes 16 rounds or cycles, each of which has simple interchanges combined with substitution in four-bit groups. In each pass, 48 key bits are selected in a pseudo-random manner from the full 56-bit key.

The problem of DES is that this prior art solution does not provide a fair
15 degree of secrecy, since for disclosure of such secret codes with possible number of 2^{64} keys combinations, substituting of all keys during a brute-force attack using modern computer techniques is performed in an acceptable time. Also, using the same plaintext and not varying the keys, produces the same encoded text. Analysis reveals the statistical regularity of the correlation between the plaintext
20 and the encoded text, and may allow decoding the encoded text without using direct substitution of all the keys.

A crypto-system using public keys RSA is described in [2] p. 37-39. This system uses a one-way function - discrete logarithms raising to a power.

GOST P. 34.11 - 94 [3], p. 3-8 discloses hatching consisting in
25 comparing an optional set of data as a sequence of binary symbols, with a short, fixed length image thereof. In this system 64-bit subwords are encoded using keys of 256 bit length.

The drawbacks of these systems are small the key length, which may permit decoding during acceptable time, and a slow decoding speed. These
30 systems are practically stable systems.

Theoretically stable systems have perfect secrecy. According to Shannon [4] p. 333-402, that means that the plaintext, and the encoded text or cryptogram, are statistically independent for all plaintext and cryptograms.

A prior art Verman crypto-system is a theoretically stable crypto-system.
35 Theoretically stable systems make certain demands on a key. For a system with

closed keys the indeterminacy of the key should not be less than the indeterminacy of the plaintext. In theoretically stable systems the length of a key should be not less than the length of the plaintext. In the Verman system the key length is equal to the length of the plaintext. This system was used in a code-notebook [5] for transfer of one encoded text. This is the main drawback of a codebook because the key should be changed and delivered with every transfer.

There are known crypto-systems using the so-called randomisers [2] p. 26 - 27. A randomiser is a software or a hardware device that encodes some symbols of plaintext with some random plurality of codes.

Typically, this is done for providing equal frequency of the plaintext alphabet. Symbol frequency equalisation is required so that a crypto-analyst cannot organise decoding of a plaintext based on analysis of frequency characteristics of a cryptogram. For a random plaintext and a random selection of a code, a derandomiser should correctly determine the initial symbol without transfer of information from the randomiser location. In classical systems with a small randomising field, this task is solved by substituting codes belonging to the randomised symbol. Randomisers, however, do not play a substantial role in crypto-protectability of an encoding system, as secret keys are the main means of protection.

Under the combination of the essential features the most close prior art object to the claimed method and device is the disclosed in [6] the device and method of encoding that use a principle of full randomizing symbols of the initial alphabet on a plurality of codes with potencies of large dimensionality, The said prior art invention was selected by the inventors for the prototype of the claimed invention.

In respect of a method the selected for the prototype object is a method of encoding and transferring information, wherein the addressee is beforehand provided for a key to the received communications with information on regularities corresponding to the values of the communication transmitted to him, with specific values of the initial information for the whole set of symbols of the said kind of an information, processing an information using the said regularities and transferring to the addressee the communication containing data, obtained during processings information, the values of transmitted data, which depend on random generated numbers being calculated during processing information, characterized in that the addressee is beforehand provided with a set of functions $Y_1...Y_n = Y_i(X)$, where X

is a variable, and each Y_i corresponds to a specific symbol of information, and also with the support function $U = U(Z)$, where Z is a variable, and with the key function $W = W(Y, U)$, where Y and U are variables accepting values of any of the values from the values of the said functions Y_i and U , in the course of processing of a transmitted information for each symbol there are generated two random numbers X and Z , the respective value of Y is calculated on basis of the respective function $Y_i(X)$ for a specific symbol, the value of U is further calculated on basis of the support function $U(Z)$, the value of W for this symbol is calculated on basis of the key function $W(Y, U)$ and obtained for the symbol value of Y and the value of U from the support function, and the addressee is transmitted the communication containing data on the thus obtained values of W , X and Z for each symbol of the initial information.

In respect of a device, the object selected for the prototype is a device for realizing a method of encoding and transferring information, which comprises a unit for information input, a set of symbols, a data base on regularities connecting the specific symbols with the communication, which data base is supplied with a calculator connected to the generator of random numbers, the device further comprising the encoder and the unit for recording and transmitting communications, and the encoder being connected to the set of symbols and calculator output, the device further comprising a unit for calculating the values of the support function and a unit for calculating the values of the key function, the generator of random numbers is supplied with two outputs joint with the encoder, the first output of the generator of random numbers is connected also to the input of the unit for calculating values of the support function, and second – to the input of the calculator of the data base on regularities, the output of this calculator is connected to the encoder through the unit for calculating values of the key function, and the second input of the latter is connected to the output of the unit for calculating values of the support function.

However the problem of object selected for the prototype is that in the course of the encryption the length of the encrypted communication exceeds the length of the initial communication by several times.

The aim of the claimed invention is providing an improved method of encrypting by means of obtaining several communications from one initial, at least one of the obtained communications may be compressed up to preset sizes so

that any connection between the initial text and the cryptogram is completely is lost for a cryptanalyst.

As a result of the solution of the problem there is achieved a new technical effect consisting in creating a new system of encrypting that ensures a high crypto-
5 stability of a system without any increase of the length of the communication.

The said technical effect is achieved as follows.

1. The method of encrypting of an information comprises the following steps:

- Preliminary generation of information on regularities connecting the values of symbols of the initial communication with the specific values of the encrypted
10 communication for the total set of values of the said kind of communications;
- determination the number (n) of transformation cycles of the initial communication;
- realization of the transformation cycle comprising:
 - generation of the feature (Ri), defining regularity used for transformation of the
15 communication in the current transformation cycle;
 - transformation of the communication with use of the selected regularity;
 - repetition of transformation cycles the certain number of times;
 - transformation of the communication in each cycle being realized in a way resulting in forming a communication (Ci), transformed in the said cycle and the
20 accessory information for the said cycle (Fi);
- the number (n) of transformation cycles of the initial communication is selected from the preset criterion,
- forming the encrypted communication consisting of two parts, one of which contains the finally transformed communication (Cn), and second one contains
25 a set of the accessory information (F = {F1, F2, ..., Fn}).

2. The further improvement of the method is characterized by that:

- transformation of the communication in each cycle is realized in a way resulting in forming a communication (Ci) transformed in the said cycle, being of the shorter or equal length with the initial communication, and resulting in forming
30 an accessory information for the said cycle (Fi);
- the number (n) of transformation cycles of the initial communication is selected from the preset criterion (for example, the size of the finally transformed communication),
- forming the encrypted communication consisting of two parts, one of which
35 contains the finally transformed communication (Cn) being of the shorter length

with the initial communication, and second one contains a set of the accessory information ($F = \{F1, F2, \dots, Fn\}$).

3. Still further improvement of the method is characterized by that:

- 5 • transformation of the communication in each cycle realizes in a way resulting in forming a communication (C_i) transformed in the said cycle, being of the shorter, equal or longer length with the initial communication, and resulting in forming an accessory information for the said cycle (F_i);
- 10 • the number (n) of transformation cycles of the initial communication is selected from the preset criterion (for example, the size of the finally transformed communication),
- forming the encrypted communication consisting of two parts, one of which contains the finally transformed communication (C_n) being of the shorter, equal or longer length with the initial communication, and second one contains a set of the accessory information (F

15

4. The further improvement of a method is characterized by that in each or some cycles the communication (C_i) transformed in the said cycle and (or) an accessory information for the said cycle (F_i) are intermixed.

5. The following improvement of the method is characterized by that in each or
20 some cycles of transformation the certain part of an accessory information for the said cycle (F_i) is added into the transformed in the said cycle communication (C_i).

The structural interpretation of stated ideas could be considered on an example of the claimed device.

25 The device for a realizing the method of encrypting information comprises:

- an input unit,
- an output unit, the first input of which is connected to the second output of the commutator, and the second — to the output of the accessory information storage ;
- 30 • data base on the regularities connecting the initial information with the encoded information, the first input of the said data base being connected to the first output of the input unit and the second input – to the output of the random numbers generator;
- a random number generator, the input of which is connected to the first output
35 of the making decision unit;

- the transformation unit, the first input of which is connected to the second output of the output unit, the second input – to the output of the data base, and the third input – to the first output of the commutator;
- the storage for the transformed information, the input of which is connected to
5 the first output of the transformation unit;
- a storage for the accessory information, the first input of which is connected to the second output of the transformation unit, and the second input – to the second output of the making decision unit;
- the making decision unit, the first input of which is connected to the third output
10 of the input unit, the second input – to the first output of the storage for the transformed communication;
- the commutator, the first input of which is connected to the second output of the storage for the transformed communication, and the second input – to the second output of the making decision unit.

15

1. The method of decoding encrypted information comprises the following steps:
 - preliminary generating data on regularities connecting values of all encoded symbols that may be used in the said kind of information with initial symbols, which are identical to the regularities used at encoding;
 - extracting, from the encoded communication, of the data (R_i), defining the
20 regularity which is used in the current transformation cycles and connects the values of the encoded communications with the concrete symbols of the transformed information of the current transformation cycle;
 - selecting the regularity connecting the values of the encoded communications
25 with the concrete symbols of the transformed information of the current transformation cycle;
 - extracting from the accessory information (F) the accessory information for the said transformation cycle (F_i);
 - transforming the transformed information (C_i) using the selected regularity and
30 the accessory information for the said transformation cycle (F_i);
 - making decision on switching to the next cycle or termination of the transformation;
 - the accessory information for the said transformation cycle (F_i); being isolated from the array of the accessory information (F);

- recovering the information (C_i), which is transformed in the respective cycle, by using the selected regularity and the accessory information for the said transformation cycle (F_i);
 - making decision on switching to the next cycle or termination of the transformation;
 - using additionally in each transformation cycle a respective part of the accessory information, as a result of transforming with the use of the selected regularity there is formed the information recovered in the respective cycle.
2. The further improvement of a method is characterized by that:
- in each transformation cycle there is additionally used a respective part of the accessory information and as a result of the transformation with use of the selected regularity there is formed a recovered in the corresponding cycle communication, the length of which is larger or equal to the length of the communication, resulting from transforming in the previous cycle.
3. The following improvement of a method is characterized by in each transformation cycle there is additionally used a respective part of the accessory information, and as a result of transformation with use of the selected regularity there is formed a recovered in the respective cycle communication, the length of which is larger, equal or smaller than the length of the communication, resulting from transforming in the previous cycle.
4. One more improvement of the method is characterized by that the transformed in the respective cycle information (C_i) and/or the accessory information for the respective cycle (F_i) is preliminary unmixed in each cycle or in some cycles;
- The device for realizing the method of decoding of the communication, comprises:
- an input unit,
 - an output unit,
 - data base on the regularities connecting the encoded information with the initial information,
 - a transformation unit;
 - a storage of the recovered communication;
 - a storage of the accessory information;
 - a making decision unit;
 - a commutator,

the first input of the accessory information storage being connected with first output of the input unit and the second input of the accessory information storage being connected with first output a making decision unit; the first input of data base is connected to the second output of the of the input unit, and the second input –
5 to the first output of the storage for accessory information; the first input of the storage of the recovered information is connected to the third output of the input unit, the second – to the output of the transformation unit, and the third – to the first output of the making decision unit, the first input of the transformation unit is connected to the second output of the storage of accessory information, and the
10 second – to the output of database, the third to the first output of the storage of recovered information; the second - to the fourth output of the input unit, the first input of the commutator is connected to the second output of the making decision unit, and the second – to the second output of the making decision unit, the output unit is connected to the second commutator output .

15 With the first output (exit) of the switchboard; the first input (entrance) of the block of a decision making is connected to the first output (exit) of an accumulator of the restored communication, and second — With the fourth output (exit) of the block of input; the first input (entrance) of the switchboard is connected to the second output (exit) of the block of a decision making, and second — With the second
20 output (exit) of an accumulator of the restored communication; the block of a conclusion is connected to the second output(exit) of the switchboard.

The distinctive feature of the new method can be illustrated by the following example. Symbols of the initial alphabet $A \{a_1, a_2, \dots, a_n\}$ being such, that the
25 binary representation of each symbol has the identical length for the whole alphabet A , are substituted with symbols of the alphabet $B_i \{b_{1i}, b_{2i}, \dots, b_{ni}\}$ being such, that the binary representation of each symbol may have a various length, the process of such replacement is iterative, i. e. at each i -step for the initial communication there is used a result of the substitution obtained at the $i-1$ step, at
30 each i -step there is used its own substitution alphabet B_i , produced with the help of the function Y_i , selected by a casual mode from a plurality of functions transferred to the addressee beforehand, and at each i -step there is produced the accessory information F_i used for restoring the initial communication is produced. As an additional measure of protecting from cryptanalysis, on each step or on
35 some steps there may be performed intermixing of the communication resulting

from the transformation. In an outcome of such transformation there is produced a transformed text (Cn), length of which may be not than the less length of one symbol of the alphabet Bn, used at the last step of transformation.

Such systems have uncommon properties:

- 5 • as a result of transformation of the initial communication there are produced at least two output communications (the transformed communication (Cn) and the accessory information (F), each of which separately has not any sense from the point of view of restoring the initial communication and may be transmitted through a separate data link;
- 10 • generally, the length of the transformed communication may have the length of one symbol of the substitution alphabet, for example if the initial communication has the byte representation, the transformed communication may have the one byte length, regardless of the length and kind of the initial communication;
- at multiple encoding one and the same initial communication the transformed communication will be various, eliminating thereby a problem of the closed channel for the key information transfer;
- 15 • The modification of any symbol in the transformed communication or accessory information brings about the impossibility of restoring the initial communication.

The transformation functions (Yi) may be preset in the form of a table. For example, in case of representing the initial communication as N-bit binary sequences and transformation of compression of the function Yi, can be preset as a set of 2^N triples — $\{(ak, bik, fik)\}$, where ak is an N-bit initial code, bik is a transformed bit code of a variable length not greater N, and only two values of {bik} have the length of N bit, fik is the information on the length of the respective bik in bits. At such representation there exist such submission exist

25 $(2^N)!(2^N - 1)(2^N - 2)$ of various possible functions of transformation such, that $\sum_{i=1}^{2^N} L_{ik} = \min L_{ik}$, where - L_{ik} - is length of bik in bits. At N = 8 there is present

30 $\approx 256! * 254 * 255 \cdot 10^{511}$ of various transformation functions (Yi). In this case two values of bik have the one bit length, four values of bik have the two bit length, eight values of bik have the three bit length, sixteen values of bik have the four bit length, a thirty two values of bik have the five bit length, sixty four values of bik have the six bit length, one hundred twenty eight values of bik have the seven bit length and two values of bik have the eight bit length.

Then for an arbitrary function Y_i the average length of the transformed communication X will be equal:

$$L(C_i(X, Y_i)) = L(X) \frac{2N + \sum_{n=1}^{N-1} n2^n}{N2^N}$$

5 and the average length of an accessory information:

$$L(F_i(X, Y_i)) = L(X) \frac{2N + \sum_{n=1}^{N-1} n2^{N-n}}{N2^N}$$

thus the average compression ratio at one step of transformation will have the values:

10

$$K_{core} = \frac{L(C_i(X, Y_i))}{L(X)} = \frac{2N + \sum_{n=1}^{N-1} n2^n}{N2^N}, \text{ for the transformed communication}$$

$$K_{flags} = \frac{L(F_i(X, Y_i))}{L(X)} = \frac{2N + \sum_{n=1}^{N-1} n2^{N-n}}{N2^N}, \text{ for the accessory information.}$$

In particular, for $N = 8$ we have: $K_{core} = 777/1024 \approx 0.758$ $K_{flags} = 255/1024$

At performing transformation M cycles the anticipated average length of the transformed communication will be:

15

$$L(C(X)) = K_{core}^M L(X),$$

and of the accessory information -

$$L(F(X)) = L(X) K_{flags} \sum_{m=0}^{M-1} K_{core}^m = K_{flags} L(X) \frac{K_{core}^M - 1}{K_{core} - 1}$$

Accordingly at performing 10 transformation cycles the average length of the transformed communication at of $N = 8$ will make approximately 0,067 of the length of the initial communication, and length of the accessory information — 0.97 of the length of the initial communication. The general length will make approximately 1.037 of the initial length, and for 100 transformation cycles — 10^{-12} and 1.04 accordingly.

25

If at each transformation cycle a S byte of the accessory information is added to the transformed communication, then average length of the transformed communication will be:

$$L(C(X)) = K_{core}^M L(X) + S \sum_{m=0}^M K_{core}^m = K_{core}^M L(X) + S \frac{K_{core}^{M+1} - 1}{K_{core} - 1},$$

And length of an accessory information will make:

$$L(F(X)) = \sum_{m=1}^M K_{flags} \left(K_{core}^m L(F) + S \frac{K_{core}^{m+1} - 1}{K_{core} - 1} \right) = \frac{K_{flags}}{1 - K_{core}} \left(L(X)(1 - K_{core}^M) + S \left(M - \frac{K_{core}^{M+2} - 1}{K_{core} - 1} \right) \right)$$

5

The construction of the claimed device may be realized in various variants realizing the claimed method of encoding information by using the known hardware. All these variants expand technological possibilities of using of the invention.

- 10 The main problem of the prototype method is eliminated thereby, i.e. essential increase of the sizes of the encrypted communication in a comparison with the initial one. The disclosed distinctive features of the claimed invention, in a comparison with known engineering solutions allow designing a device of encoding information providing statistical independence of the encrypted text and
- 15 the open text, i.e. having properties of the theoretically stable of proof system of cryptography, and not by recurrence of the encrypted communication at repeated encoding of one and the same communication at constant keys.

Fig.1 shows a diagram of the device illustrating realization of a claimed method of encoding information is represented. Through the input unit the data

20 base enters the pre-generated information on regularities connecting values of symbols of the initial communication with specific symbols of the encrypted communication for the whole set of symbols of the said kind of the communications. In the course of processing the encrypted information the input of the making decision unit (3) enters the information on the number (n) of

25 transformation cycles of the initial communication. Before the beginning of the current transformation cycle, the making decision unit (3) transmits a control signal to the generator of random numbers (5), which generates a random number (Ri), transmits it to the data base (2) and through the latter- to the transformation unit. In accordance with the value of Ri from the database (2) there is selected the

30 transformation function of YRi which enters the transformation unit (4). The transformation unit (4) calculates s the values of (Ci, Fi) = YRi (Xi, Ri). The value of Ci enters the input of the storage of the transformed communication (6) from outputs of the transformation unit (4) and the value of Fi enters the input of the

storage of the accessory information (7). The storage of the transformed communication (6) transmits a signal on termination of the current cycle of transformation to the making decision unit (3). The making decision unit (3) makes a decision on fulfillment of the next transformation cycle or on terminating the process of transformation. In case of decisionmaking on the terminating the process of transformation the transformed information (C_n) through the switchboard (8) and the accessory information $F = \{F_1, F_2, \dots, F_n\}$ from the storage of an accessory information (7) enters the output unit (9). Otherwise the transformed communication (C_i) through the switchboard (8) enters in the transformation unit (4) for fulfillment the next cycle of transformation.

Fig. 2 shows the diagram of the device illustrating realization of the claimed method of decoding information. Through the input unit (10) into the data base (2) come the previously generated information on regularities connecting values of symbols of the initial communication with special symbols of the encrypted communication for the whole set of symbols of the said kind of the communications, which are identical to the regularities used at encoding. In the course of restoring the transformed communication through the input unit (10) enter the following data: at the input of the decision making unit (11) - information on the number (n) of transformation cycles of the deencrypted communication; at the storage of the accessory information (14) - the accessory information; at the storage of the restored communication (13) - the transformed communication. Before the beginning of the current cycle of restoring at the signal of the decision making unit (11) the storage of the accessory information (14) yields the accessory information (F_i) into the transformation unit (12) and the value of R_i - into the data base (2), in accordance with which is selected the function of transformation of Y_{Ri} that arrives at the transformation unit (12), and the storage of the restored communication (13) yields through the switchboard (8) the transformed communication (C_i) into the transformation unit (12). The transformation unit (12) calculates the values of (X_i) $Y_{Ri}(C_i, F_i)$. From the output of the transformation unit (12) the restored communication (X_i) arrives into the storage of the restored communication (13). At completion of accumulation of the restored communication (X_i) the storage of the restored communication (13) sends a signal on termination of the current cycle of restoring into the decision making unit (11). In case of decision-making on the termination of process of transformation the restored

communication (Xi)) through the switchboard (8) arrives to the output unit (15). Otherwise from the output of the decision-making unit (11) at the input of the storage of the accessory information (14) arrives the signal on yielding of the next portion of the accessory information (Fi, Ri) and the restored communication
5 arrives through the switchboard (8) at the transformation unit (12) for fulfillment of the next cycle of restoring.

Bibliographic data of sources of information

10

1. Victor Gavrish "Practical Guide on Protecting Commercial Secrets". Simferopol, TAVRIDA, 1994, p.35-37.
2. . Schmidt M. E., Bransted D.K. "Standard of Data Encoding: Past and Future" Journal of Works of Electronic and Radio Engineers (TIER), 1988, v.76, no. 5.,
15 p. 33-34.
3. GOST 34.11-94 Information Technology, Crypto Graphical Protection of Information, Cash function. M.: Gosstandart of Russia, 1994, 34.11 - 94, p. 3-8.
4. Shannon C. E.. "Communication Theory in Secret Systems". Shannon C. E. "Works on Information and Cybernetics Theory". M.: IL, 1963, p. 333-402,
20 "Theoretically Stable system," as cited in "An Introduction to Contemporary Cryptology", Proceedings of the IEEE, v. 76. No. 5, May 1998.
5. Vernan. Copher printing telegraph systems for secret wire and radio telegraphic communications. // J Amer. Inst. Elec. Eng., vol. 55, pp. 109-115, 1926.
6. Mischenko V.A, Zakharov V.V. A method of encoding and transfer information
25 and the device for a realization the method // Official Gazette of the Belarusian Patent Office. No.4, part I, 1997
7. Golubev V.V. Computer crimes and protection of information in computing systems // News in life, science and engineering. Part. Computer engineering and use thereof. Protection of information.- M.: Znanie, 1990.

30

Claims

1. A method for encoding information comprising the steps of:
 - preliminary generating data on regularities connecting values of all initial symbols that may be used in the said kind of information with encoded symbols;
 - 5 - determining the number (n) of cycles of transforming specific initial information;
 - realising the cycle of transforming which comprises:
 - generating the feature (R_i) that determines the regularity used for transforming the information in the current transformation cycle;
 - 10 - transforming the information using the selected regularity;
 - repeating transformation cycles a certain number of times;
 - *characterised in that,*
 - transforming of the information in each cycle is performed in such a way that results in forming a transformed in the said cycle information (C_i) and the
15 accessory information for the said cycle (F_i);
 - the number (n) of cycles of the transformation of the initial information is selected from the preassigned criterion,
 - forming an encoded message consisting of two parts, one of the said parts comprises the finally transformed information (C_n), and the second one
20 comprises the accessory information array ($F = \{F_1, F_2, \dots, F_n\}$).
2. The process for encoding information according to claim 1, *characterised in that*
 - transforming the information in each cycle is performed in such a way that
25 results in forming a transformed in the said cycle information (C_i), that is shorter or equal to the length of the initial information, and the accessory information for the said cycle (F_i);
 - the number (n) of cycles of the transformation of the initial information is selected from the preassigned criterion determining the size of the finally transformed information,
 - 30 • forming an encoded message consisting of two parts, one of the said parts comprises the finally transformed information (C_n) that is shorter than the length of the initial communication, and the second one comprises the accessory information array ($F = \{F_1, F_2, \dots, F_n\}$).
3. The process for encoding information according to claim 1, *characterised in that*
35

- transforming the information in each cycle is performed in such a way that results in forming a transformed in the said cycle information (C_i) that is shorter, equal or longer than the length of the initial information and the accessory information for the said cycle (F_i);
- 5
- the number (n) of cycles of the transformation of the initial information is selected from the preassigned criterion, determining the size of the finally transformed information and/or the degree of protectability of information,
 - forming an encoded information consisting of two parts, one of the said parts comprises the finally transformed information (C_n) that is shorter, equal or
- 10
- longer than the length of the initial communication, and the second one comprises the accessory information array ($F = \{F_1, F_2, \dots, F_n\}$).
4. The method according to claims 1, 2 or 3, *characterised in that* the transformed in the said cycle information (C_i) and/or the accessory information for the said cycle (F_i) are mixed in each cycle or in some cycles.
- 15
5. The method according to claims 1, 2, or 3, or 4, *characterised in that* the certain part of the accessory information for the said cycle (F_i) is added to the transformed in the said cycle information (C_i) in each or some transformation cycles.
6. The device for realising the process for encoding of information, comprises:
- 20
- an input unit,
 - an output unit, the first input of which is connected with the second output of the commutator, and the second — with the output of the accessory information storage ;
 - data base on the regularities connecting the initial information with the encoded
- 25
- information, the first input of the said data base being connected with the first output of the input unit and the second input – with the output of the random numbers generator;
 - *characterised in that*, the device further comprises
 - a random number generator, the input of which is connected with the first output
- 30
- of the making decision unit;
 - the transformation unit, the first input of which is connected with the second output of the output unit, the second input –with the output of the data base, and the third input –with the first output of the commutator;
 - the storage for the transformed information, the input of which is connected with
- 35
- the first output of the transformation unit;

- a storage for the accessory information, the first input of which is connected with the second output of the transformation unit, and the second input – with the second output of the making decision unit;
 - the making decision unit, the first input of which is connected with the third
5 output of the input unit, the second input – with the first output of the storage for the transformed communication;
 - the commutator, the first input of which is connected with the second output of the storage for the transformed communication, and the second input – with the second output of the making decision unit.
- 10 7. The process for decoding of the encoded information comprising the steps of:
- preliminary generating data on regularities connecting values of all encoded symbols that may be used in the said kind of information with initial symbols, which are identical to the regularities used at encoding;
 - extracting , from the encoded communication, of the data (R_i), defining the
15 regularity which is used in the current transformation cycles and connects the values of the encoded communications with the concrete symbols of the transformed information of the current transformation cycle;
 - selecting the regularity connecting the values of the encoded communications with the concrete symbols of the transformed information of the current
20 transformation cycle;
 - extracting from the accessory information (F) the accessory information for the said transformation cycle (F_i);
 - transforming the transformed information (C_i) using the selected regularity and the accessory information for the said transformation cycle (F_i);
 - 25 • making decision on switching to the next cycle or termination of the transformation;
 - *characterised in that*, the accessory information for the said transformation cycle (F_i); is isolated from the array of the accessory information (F);
 - recovering the information (C_i), which is transformed in the respective cycle, by
30 using the selected regularity and the accessory information for the said transformation cycle (F_i);
 - making decision on switching to the next cycle or termination of the transformation;

- using additionally in each transformation cycle a respective part of the accessory information, as a result of transforming with the use of the selected regularity there is formed the information recovered in the respective cycle.
8. The process of decoding the encoded information according to claims 7,
5 *characterised in that*
- in each transformation cycle there is additionally used a respective part of the accessory information and as a result of transformation with use of the selected regularity there is formed a recovered in the corresponding cycle communication, the length of which is larger or equal to the length of the
10 communication, resulting from transforming in the previous cycle.
9. The process of decoding the encoded information according to claims 7,
characterised in that
- in each transformation cycle there is additionally used a respective part of the accessory information, and as a result of transformation with use of the
15 selected regularity there is formed a recovered in the respective cycle communication, the length of which is larger, equal or smaller than the length of the communication, resulting from transforming in the previous cycle.
10. The method according to claims 7, 8 or 9, *characterised in that*, the transformed in the respective cycle information (C_i) and/or the accessory
20 information for the respective cycle (F_i) is preliminary unmixed in each cycle or in some cycles;
11. The device for realising the process for decoding information, comprises:
- an input unit,
 - an output unit,
 - 25 • data base on the regularities connecting the encoded information with the initial information,
 - *characterised in that*, the device further comprises
 - a transformation unit;
 - a storage of the recovered communication;
 - 30 • a storage of the accessory information;
 - a making decision unit;
 - a commutator,
- the first input of the accessory information storage connected with first output of the input unit and the second input of the accessory information storage connected
35 with first output a making decision unit; the first input of data base is connected to

the second output of the of the input unit, and the second input – to the first output of the storage for accessory information; the first input of the storage of the recovered information is connected to the third output of the input unit, the second – to the output of the transformation unit, and the third – to the first output of the making decision unit, the first input of the transformation unit is connected to the second output of the storage of accesory information, and the second – to the output of database, the third to the first output of the storage of recovered information; the second - to the fourth output of the input unit, the first input of the commutator is connected to the second output of the making decision unit, and the second – to the second output of the making decision unit, the output unit is connected to the second commutator output .

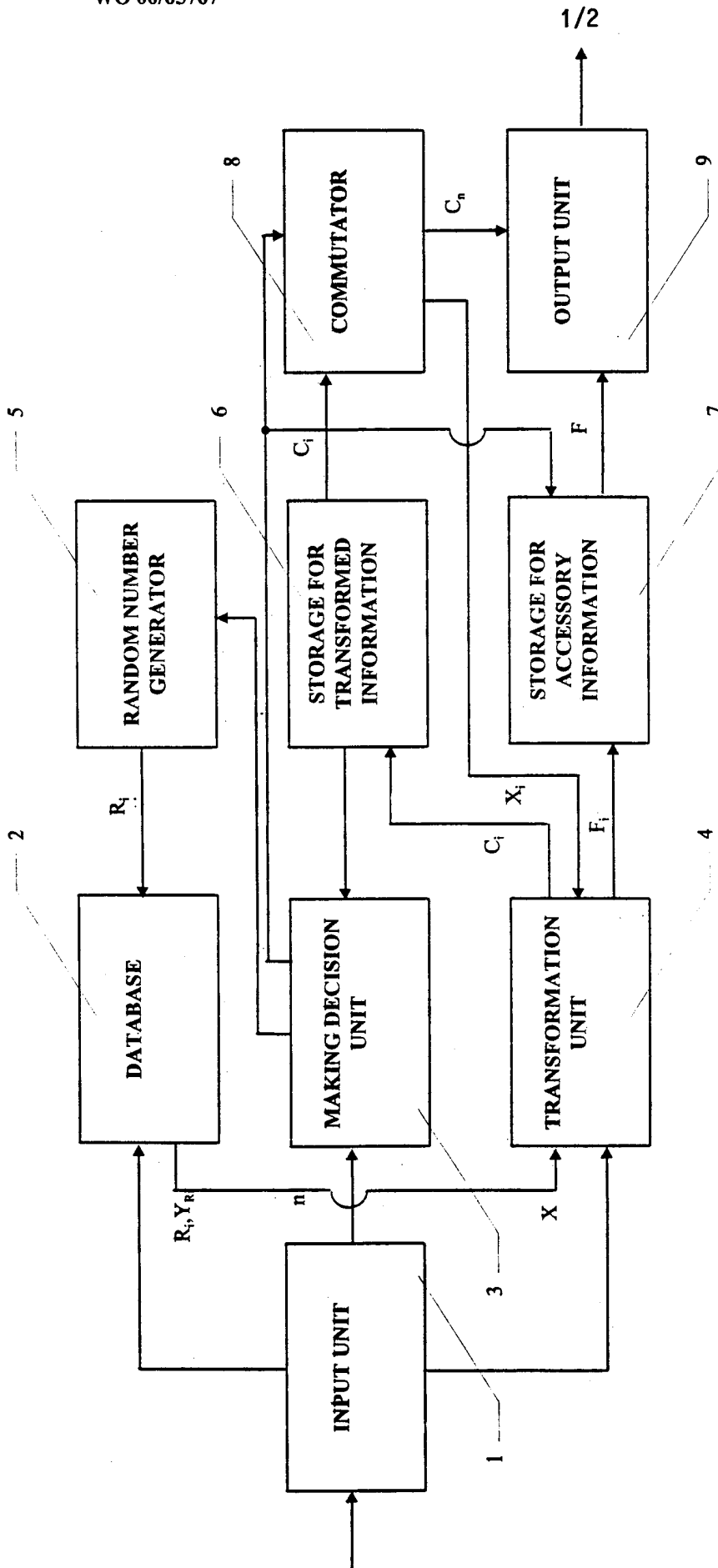


FIG 1

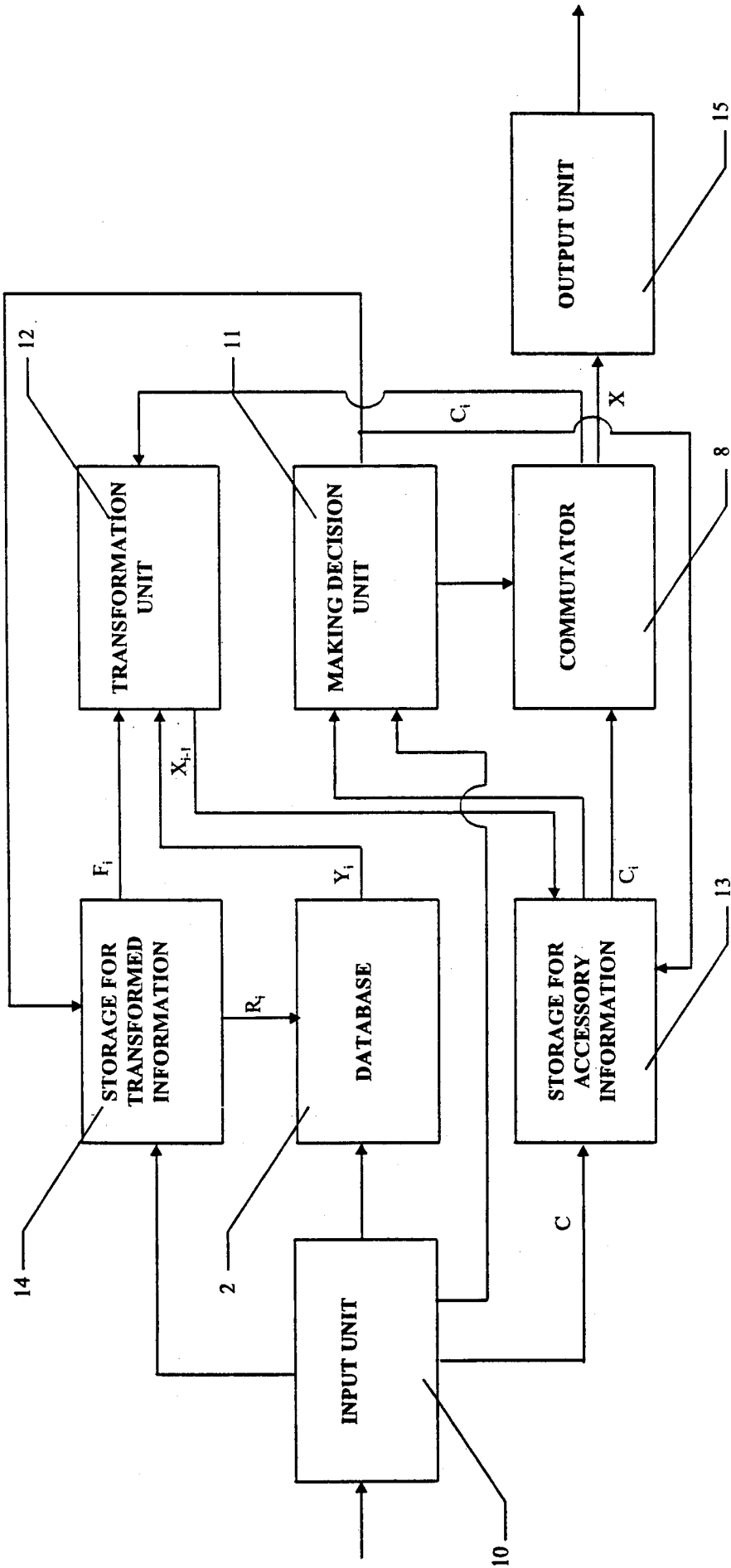


FIG. 2

INTERNATIONAL SEARCH REPORT

Interr 1al Application No

PCT/BY 99/00005

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 222 139 A (TAKARAGI ET AL.) 22 June 1993 (1993-06-22) column 2, line 55 - line 63 column 3, line 9 - line 27 column 8, line 41 - line 55 -----	1,6

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

12 January 2000

Date of mailing of the international search report

20/01/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Authorized officer

Holper, G

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/BY 99/00005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5222139 A	22-06-1993	JP 4170576 A	18-06-1992