*Journal of Engineering Science* *Vol. XXVIII, no. 1 (2021), pp. 75 - 82*
*Fascicle* *Electronics and Computer Science* *ISSN 2587-3474*
*Topic* *Computers and Information Technology* *eISSN 2587-3482*

**https://doi.org/10.52326/jes.utm.2021.28(1).07**
**UDC 004.056.55:004.421**

# SPECTRAL SPACE AS A METHOD FOR DATA CRYPTO PROTECTION USING THE FAST FOURIER TRANSFORM

Anatoly Balabanov, ORCID ID: 0000-0003-1225-8247,
Vyacheslav Kunev, ORCID ID: 0000-0002-1095-214X,
Victor Colesnic*, ORCID ID: 0000-0001-8675-4062

Technical University of Moldova, 168 Stefan cel Mare bvd., MD-2004 Chisinau, Republic of Moldova
*Corresponding author: Victor Colesnic, *victor.colesnic@ati.utm.md*

Received: 01. 05. 2021
Accepted: 02. 17. 2021

**Abstract.** The article proposes to solve the problem of real-time application (on-line) of asymmetric bit-by-bit (flow or phoneme block, 32-, 64-,..., n-bits block) encryption of the linear and / or non-linear formants of the spectrum lines of Fast Fourier Transform (FFT) as an indirect analogue of a voice message. For this, modernized RSA-m algorithms are used and the spectrum of the voice message in the form of linear formants of number theory, while maintaining the high level of cryptographic resistance inherent of the RSA algorithm. The peculiarity of these algorithms consists in the fact that different lengths of cryptographic keys are used, which are changed with a sufficient frequency, depending on the required level of cryptographic resistance. This feature of the algorithms implements statistically independent encoding of the original message, by encrypting the adequate formants of the original message, i.e. a process characterized by a reduction (compression) of the amount of initial information and its redundancy, as well as an increase of its entropy (the average amount of information per character, phoneme or discrete (n-bit output from the ADC), because in a compressed context, statistically frequent sounds, letters, words, phonemes and even discrete, will be absent, which will significantly complicate the decryption (cryptanalysis) of the message.

**Keywords:** *cryptographic systems, online encryption, RSA modernization, RSA-m algorithms, formant analysis, cryptographic resistance.*

## Introduction

Any signals are - from the point of view of Fourier - an infinite sum of sinusoids of different amplitudes, frequencies and phases, which means, according to his famous Theorem - just some sequence of discrete (spectral lines) in the spectral space. And any text (or media data), as you know, can also be represented in a binary digital space - as a protocol, known in advance, some sequence of ones and zeros in the time (frequency) domain, i.e. also as a possible binary representation of any information, including (why not!) spectrum of some random signal consisting of 1 and 0!

The term "space" should not discourage the cryptographer, since reality and abstraction from it are natural in mathematics. However, the physical perception of these operations cannot always be adequately assessed immediately. The algorithmic and mathematical procedures, methods and operations described below relate to the field of mathematical and logical-algorithmic space in the field of cryptographic transformations and protection of confidential and / or stored information transmitted bit by bit or in batches, for use in computing and information systems, in local corporate networks, in radio communication systems, information and control complexes, in systems of mass mobile (cellular) telephony, confidential telephone digital communication of state, commercial, security and signaling enterprises and financial structures, as well as in devices such as the "global messenger" for encryption of binary information.

The listed devices must contain on the transmitting and receiving sides a speech converting devices (SCD) connected via a USB port or a wireless Bluetooth port, Wi-Fi, WiMax and the like to a radio, mobile and telephone communication device (smartphone, iPhone, tablet, etc. other existing or possible similar devices in the future) or to any other radio transmitter, which must contain an encryption unit between the SCD output and a mobile and other radio or telecommunication device, which implements algorithms for closing and protecting information in the online mode.

Today, dozens of patent methods and corresponding devices for cryptographic information protection are known [1 - 11]. These systems are characterized by the complexity of algorithms, operations, rather slow execution and insufficient cryptographic strength when receiving / transmitting online, which becomes especially noticeable in the conditions of post-quantum cryptography. Therefore, in the method described below, one of the tasks to be solved is associated with increasing the cryptographic strength.

An essentially similar method for encrypting binary information and a device based on it are described in [12], which describes a method for cryptographic protection of information in computing and information systems. It is based on encrypting digital, usually 64-bit blocks, using two keys - public and private, and is based on the use of one-way functions and arithmetic of large numbers. This method takes the computational complexity of the problem of factorizing a large number into prime factors (finding the divisors of a large number) in a reasonably short time. The disadvantage of this cryptosystem is the inability to influence the spectral characteristics of the transmitted information in the desired way.

**The tasks and goals set**

The aim of the present invention **is to apply in real time** (on-line) asymmetric bit-by-bit (streaming or block-phoneme, block on 32-, 64-, n-bit) **encryption of the linear and / or non-linear formants of the spectrum lines of Fast Fourier Transform** (FFT) as an indirect analogue of a voice message. For this, modernized RSA-m algorithms [12, 13] are used and **the spectrum of the voice message in the form of linear formants as a mathematical image** [14] (model, convolution), while maintaining the high level of cryptographic resistance inherent in the RSA algorithm. The peculiarity of these algorithms is that short lengths of crypto-keys are used, varying with a sufficiently high frequency, providing a short-term level of protection for conversations (3 - 10 minutes), and with an increase the level of long-term security (up to several months and years), the lengths of crypto keys are additionally changed to values that provide the required level of cryptographic strength.

This feature of the algorithms that implements the process of statistically independent coding of the original message by encrypting its adequate formants, i.e. the process characterized by a decrease (compression) in the volume of initial information and its redundancy, as well as an increase in its entropy (the average amount of information per symbol, phoneme or discrete), because in a compressed context, **statistically frequent sounds, letters, words, phonemes and even discrete will be absent**, **which will significantly complicate the decryption (cryptanalysis) of the message.** Objectives - improving the quality of cryptographic information processing, i.e. speed and stability of various durations of secrecy, increasing the speed of the encryption / decryption procedure by reducing the amount of information in an encrypted M-bit message, as well as expanding the functionality and application areas of the proposed method for protecting binary information.

Based on the rule of A. Kerckhoff (1835-1903): " a cryptographic system should be designed to be secure, even if all its details, except for the key, are publicly known", in the claimed method for encrypting binary information during its transmission over an open channel, not the original information is transmitted, but its image, an adequate model, i.e. some not obvious information about it, known only to the receiving party, or the internal software of the encryption device, based on which the original information can be easily restored. To do this, use, for example, one- or two-dimensional numerical formant [14], whose values change in time depending on the value of the digital representation of the protected information. The formant itself is transmitted encrypted using the RSA-m algorithm or some other, for example, a hybrid algorithm.

## The essence of the encryption method

The essence of the method for encrypting binary information is to use the properties of the formant [13, 14] and the RM patent No. 4511, where any number can be uniquely represented as three small numbers (**in the case of a linear formant**), significantly smaller in absolute value than the original large number, **or a greater number of them in the case of using a two-dimensional formant.** Time of encryption and decryption of a large number formant, i.e. its parameters, declared by the RSAm algorithms, are much less than the time of encryption and decryption of the original large number, which is, for example, a 32-bit or 64-bit digital block in the classical RSA cryptosystem. The advantage of the formant representation of numbers for encryption is that the base of the formant can be any number, and simple and composite, which significantly increases the number sets for choosing a formant base for encryption (which increases the cryptographic strength of the algorithm) and for hacking it during crypto analysis which complicates this task for the attacker, for example, in the interval 2-3560 there are only 500 primes, i.e. 7 times less than all the numbers in the series.

Prime formants have a number of features [12 - 14] that are important for the RSA algorithm. In the inventive method, either only two parameters of the **nonlinear formant** are encrypted, or already encrypted formants are selected from the ROM according to a given algorithm (depending on the chosen method of protecting information), **and in the case of a two-dimensional formant, only a part of the formant is encrypted, the recovery of which is possible only on the receiving side using the second secret half of the formant, which does not participate in the formation of the encrypted information transmitted over the communication channel.**

For encryption, in the device under consideration, *KN* matrices of size $n \times n$ are created to store the module numbers $N = p'q'$, calculated in accordance with the Fermat algorithm based on the primes $p'$ $and$ $q'$ of RSA encryption and pre-selected pairs of crypto-keys $e_i$ $and$ $d_i$ with different length $\mu(s_i)$ bit, and $\boldsymbol{PF}$ matrix to storage bases $p_i$, cores $k_i$ and remainders $q_i$ of formants corresponding to the open message code and an $n \times n$ R matrix for storing M-bit random bit sequences for encoding encrypted blocks of information.

In the process of broadcasting a conversation through a communication channel figure 1, (radio, mobile phone, Internet, etc.), each discrete at the ADC output (2) with an amplitude $A_d(t_i)$ bits is considered as the address of the location of crypto-keys located in ROM (4) in PF matrices with a volume of $2^{32}$, where crypto-keys are randomly distributed to addresses, i.e. the matrix address does not match the discrete value.

Encryption is performed in two stages:

1) finding the formant parameters - the core $k_i$ and the remainder $q_i$ for the next amplitude $A_d(t_i)$ of the discrete (block phoneme) on the base $p_i$;

2) encryption by the RSAm algorithm of the formant parameters $k_i$ and $q_i$ on modulo $N_i$ with their own individual crypto-key $e_i$. (i-number of the encrypted / decrypted discrete or information block, according to the asymmetric RSA cryptosystem algorithm $e_i d_i (modN) = 1$).

After each communication session, the key addressing in the ROM is automatically changed according to the software algorithm. Thus, the proposed method is actually equivalent to encrypting a message with a one-time key with a random length equal to the length of the bits of the discrete or block (depending on the selected algorithm), which corresponds to the conditions of Shannon's theorem on the impossibility of decrypting [12,14]. The use of hardware implementation will provide increased encryption speed.

Difference of the proposed algorithm from its analog [12] **is that not the real digital information at the microphone output is encrypting, but its spectral representation as a result of the discrete FFT of an online message** with its encryption based on algorithms for the formant representation of FFT-transformed information.

The set goals and results are achieved through the use of: 1) RSA algorithms in real time (on-line) with significantly shortened crypto key lengths and 2) fast algorithms for fetching from memory, pre-generated, random bit sequences with the declared cryptographic strength of the information security system **to increase the speed of operation, productivity, usability and a significant expansion of application areas** for protected technologies. The method for encrypting binary information is implemented on the basis of combining blocks and devices for converting, encoding and cryptographic processing of information into a single system, communication channels and at the same time, the device itself for cryptographic information processing is made as a channel, and there are at least two of them.

***Abbreviations and symbols used in the text and in Figure 1:*** **SCD** (1) – speech converting devices, **ADC** (2) - analog-to-digital and **DAC** (13) - digital-to-analog converters; **ROM** (4) - read-only memory; **SO** - software; **CD** (4) - computing device and software; **BGP** (7) - block for generating and processing service information; **MC** - microcontroller; $\boldsymbol{k, l}$ - number of bits of crypto-keys $\boldsymbol{e_i, d_i}$ of encrypted and decrypted messages; $\oplus$-logical operation modulo 2 addition; encryption algorithm **RSA** - using large numbers for crypto keys $\boldsymbol{e_i, d_i}$ and for module **N**; modernized encryption algorithm $\boldsymbol{RSAm - ABi}$ - using small numbers for crypto keys $\boldsymbol{e_i}, \boldsymbol{d_i}$ and for module **N**, but with a high frequency of their change; $\boldsymbol{N = p'q'}$ - the multiplication of small coprime numbers chosen according to Fermat's theorem; $\boldsymbol{A_m(t_i)}$ — amplitude of the current discrete $\boldsymbol{D_i}$ of the message $\boldsymbol{S_0}$; $\boldsymbol{KN}$ – matrix of addresses of parameters of the current crypto-lock: pair of crypto keys $\boldsymbol{e_i}, \boldsymbol{d_i}$ and module $\boldsymbol{N_i}$; $\boldsymbol{PF}$ - matrix of formant parameters: base $\boldsymbol{p_i}$ of formant; core $\boldsymbol{k_i}$ and remainder $\boldsymbol{q_i}$; $\boldsymbol{R}$ — a matrix of random $\boldsymbol{M}$ —bit numbers (random bit sequences), where $\boldsymbol{M}$ is the length of the transmitted message to the open communication channel; phoneme or block phoneme - a set of discrete from several 4, 6 or 8 bytes, considered as a bit integer.

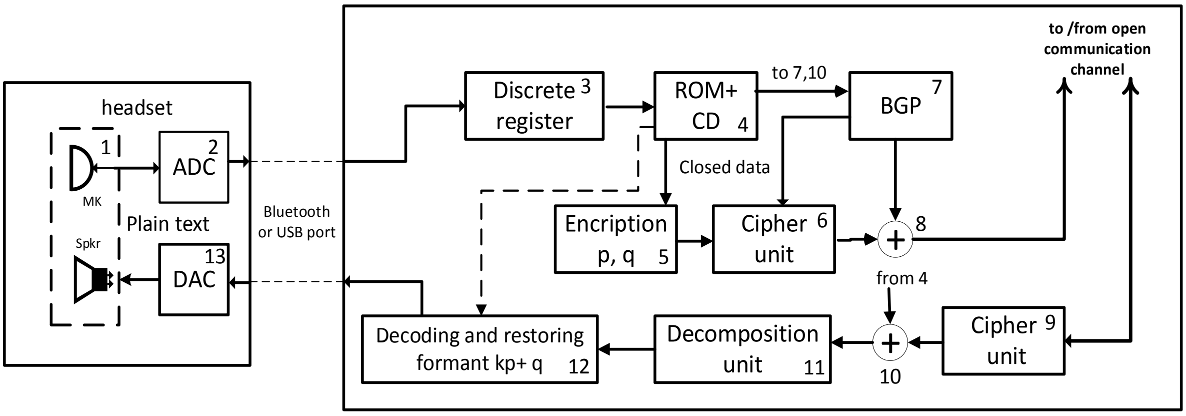

**Figure 1.** Block diagram of the encryption and decryption device.

In the information transmission path Figure 1, after the ADC (2), which converts the analog electrical signal of sound, speech into digital form from the output of the speech converting devices SCD (1), form digital n-bit blocks of the information part and auxiliary components for bitwise encryption of each discrete of the digital block based on the methods of formant analysis [13, 14]. Each such protected information block is transmitted to the communication channel in packet form using the discrete register (3), a computing device (4) and a read-only memory device (ROM) (4), which, after formant converter (5), an cipher unit (6), and a generator of a random M-bit bit sequence for noise immunity of a message from the BGP output (7), summed up modulo 2 in block (8).

In the information receiving path, encrypted coded packets are restored in communication channels using a cipher block (9), a decoder (10), block of decomposition into information and auxiliary parts (11), decryption of information blocks and restoration of the formant of the signal spectrum in block (12) based on formant analysis algorithms using the program for controlling the operation of CD blocks (4) of microcontrollers at the receiving and transmitting sides, which is an informational and technical result, with the restoration of a continuous analog speech signal based on a speech converting devices (1) connected to the output of a digital-to-analog converter DAC (13), which converts a decoded digital signal into an analog one.

The considered method of encrypting information is based on the transmission *not of the signal spectrum (the information itself), but some special indirect information about the signal spectrum, called a formant or image, model, convolution,* etc., the volume of which is significantly less than the original and, therefore, can be transmitted in encrypted form in real time (on-line) with the required level of cryptographic strength based on the "classical" algorithm of the asymmetric RSA cryptosystem.

The proposed method of encrypting information differs from the known, in that it is actually equivalent to practical message encryption with a one-time key with a random length equal to the bit length of a discrete or a block (depending on the chosen algorithm) **using real-time encryption**, which corresponds to the conditions of Shannon's theorem on the impossibility of decryption [12,14].

Indeed, block encryption can be done in two ways:

**Without feedback loops** (FL), when several bits - one discrete or phoneme - a block, for example, from 12 bit - of the original text (digitized speech by a 12-bit ADC) are encrypted sequentially, and each bit of the original block affects each bit of the cipher text. However, there is no mutual influence of the blocks (the previous discrete does not affect the next one and vice versa), that is, two identical blocks of the original text (but not speech) would be represented by the same ciphertext. Therefore, such algorithms can only be used to encrypt a random sequence of bits. Using formants (parameters - base $p_i$, core $k_i$ and remainder $q_i$) this is not the case.

**The same sequence of bits will be represented by different cipher text**. In other words, the proposed encryption method will provide statistical independence of open messages and cryptograms. But, as in the case of polyalphabetic substitutions, since the set of used formant bases is not infinite, then after a certain number of blocks they will have to be used again. Note that when randomly using numbers for base of formants, such an incident can occur, but quite rarely. Indeed, 11000 discrete / sec (the sampling of the analog signal is performed at a frequency of 11 kHz) in the presence of 10,000 different variants of the bases of the formant, will give a very small probability of coincidence of 2 encrypted texts even with monotonous sound - an ideal sinusoid:

$$p_{sovp} = \left(\frac{2}{11000}\right) \cdot \left(\frac{1}{10000}\right) = 0{,}18 \cdot 10^{-3} \cdot 10^{-4} = 18 \cdot 10^{-9} \quad (1)$$

Then 3 minutes = 180 seconds of a digitized conversation represent

$(11 \cdot 10^3) \cdot 180 = 198 \cdot 10^4 \approx 2 \cdot 10^6$ discrete, and the probability of coincidence of two identical discrete with their cipher texts will be

$$18 \cdot 10^{-9} \cdot 2 \cdot 10^6 = 36 \cdot 10^{-3}.$$

But even such a relatively low probability of coincidence of two bits on a time interval of 3 minutes does not mean anything, because we are talking about only one discrete, and in order to distinguish a sound (or even an alphabet symbol), you need a well-defined sequence of not two, but sets of samples (from several hundred to thousands!). Then the probability of coincidence of two cipher symbols or, moreover, cipher phonemes, decreases due to the appearance of huge quantities of a combinatorial nature in the denominator of formula (1), since for a text symbol this probability of coincidence of two discrete (phonemes) $p_{sovp} = \mathrm{C}_{10^2}^{10^{-9}} \approx 10^{-80}$, , and for the phoneme of sound, the number of permutations will have to be counted even 10 times more, i.e. for a phoneme, the probability will decrease to the order of

$$\mathrm{C}_{10^3}^{10^{-9}} \approx 10^{-800}.$$

Astronomically small numbers! Therefore, the probability of hacking on the basis of statistical analysis of the text cipher with the proposed encryption method is reduced to almost zero.

As a figurative explanation of the complexity of hacking this cipher by the "brute force" method, we can give an example from the famous TV game "Guess the melody", when a game participant needs to guess the melody by three consecutive sounds or notes. Note that the digital representation of the "task" to the guessing person means (represents) not 3 (three) consecutive correct discrete, but the correct sequence, at least $33 \cdot 10^3$ discrete provided that the sound is sampled at a frequency of 11 kHz!

It is clear that it is impossible to recover the necessary melody, even known in memory, from three discrete in a reasonably short time, even when using a high-speed computing (a quantum computer, for example!).

In another, much simpler the game "Guess the Word", where you need to reconstruct an unknown word of length N letters from 3 … 4 letters. In this case, the computer finds a solution in a split second. What is the difference? The number of different sorting options and known / unknown " full original"). When recognizing unknown music, the number of options is the same, but the time of hacking is infinite, if the Man himself is not involved or some model of artificial intelligence is not involved in the process of recognizing an unknown melody or speech. But encrypted messages (speech, text, image, video and other media information) are unknown in advance.

**Encryption with FL** is usually organized to increase noise immunity as follows: the previous encrypted block is added modulo 2 with the current block. The initialization value is used as the first block in the FL chain. An error in one bit affects two blocks - the erroneous and the next one.

## Conclusions

In the proposed method for encrypting binary information using RSA_mAB algorithms, the transmitted encrypted FFT packet is additionally encoded with the "xor" cipher before being sent to the communication channel.

Therefore, to break the cipher, an attacker will first have to decode this cipher packet and after decrypt each spectral line (discrete) of the spectrum, which will require additional time and may significantly overlap the guaranteed secrecy period, after which all encryption data will already be deleted from the system

Using a fully hardware implementation, not software, of the microprogram machine would provide a higher encryption speed.

### References

1. GOST 28147-89. [Information processing systems. Cryptographic protection. Cryptographic transformation algorithm], http://docs.cntd.ru/document/gost-28147-89 [in Russian].
2. Moldovyan A.A., Moldovyan N.A., [Method for block iterative encryption of binary data], https://findpatent.ru/patent/221/2212108.html [in Russian].
3. Guts N.D. i dr., [Iterative Block Cipher Method], https://findpatent.ru/patent/217/2172075.html [in Russian].
4. Klepov A.V., [Method for cryptographic protection of information in information technologies and a device for its implementation], https://findpatent.ru/patent/220/2206182.html [in Russian].
5. Chizhukhin G. N., [Method for encrypting binary information and device for its implementation], https://findpatent.ru/patent/209/2091983.htm [in Russian].
6. Volkov S. S. i dr., [Method for encrypting binary information and device for its implementation], https://findpatent.ru/patent/209/2096918.html [in Russian].
7. Averin S. V. i dr., [System of secret transmission and reception of voice information], https://findpatent.ru/patent/209/2099885.html [in Russian].

8. Lysenko V. V. i dr., [Mobile information security device with an increased level of security], http://poleznayamodel.ru/model/8/83861.html [in Russian].
9. Lysenko V. V. i dr., [Mobile information security device], http://poleznayamodel.ru/model/8/83862.html [in Russian].
10. Fodorov i dr., [Encryption-decryption device], patent RF № 2108002 http://www.findpatent.ru/patent/210/2108002.html [in Russian].
11. Khrenov V. P., [Information security system], patent RU 2 325 6956 http://www.freepatent.ru/images/patents/140/2325695/patent-2325695.pdf [in Russian].
12. Balabanov A. A., Dispositiv şi procedeu de protecţie criptografică a informaţiei binare (variante) [Device and method for cryptographic protection of binary information (variants)], patent RM №4511, 2016.04.20
13. A.A. Balabanov, A.F. Fodorov, I. Kozhukhar. [Possibilities of creating new and modernized algorithms for the RSA system]. Vestnik nauchno-tekhnicheskogo razvitiya, VNTR, №9 (37). Sept. 2010, http://vntr.ru/ftpgetfile.php?id=451 [in Russian].
14. Agafonov A.F., Balabanov A.A., [Comparative analysis and its applications. Modern and classical problems of number theory and cryptography] ,Ed., LAP Lambert Academic Pudlishing, Germany, 201 c., ISBN 978-3-659-92621-1, 2016 [in Russian].