computing@tanet.edu.te.ua
www.tanet.edu.te.ua/computing

ISSN 1727-6209
International Scientific
Journal of Computing

FAST ALGORITHMS AND COMPUTING MEANS OF CRYPTOLOGICAL FUNCTIONS

Andriy Horpenyuk

National University “Lviv Politechnic”, Ukraine, andchifp@yahoo.com

Abstract: *The problems of speed of asymmetric cryptology computational algorithms are analyzed in the article. There has been offered for the greater speed to apply computing facilities of analytical principle of functioning together with algorithmic computing facilities. There have been given fundamentals of synthesis of such facilities, considered problems that limit domain of their application in cryptography. There have been given research results, which expose the prospects of application domain expansion of such facilities.*

Keywords: – *asymmetric cryptology, encryption, decryption, cipher opening, digital differential analyzer, digital integrator, digital analogues, pulse-number functional converter.*

1. INTRODUCTION

It is known that in the second half of the twentieth century a new direction in cryptology was started that is asymmetric cryptology [1,2]. The asymmetric algorithms of encryption allowed the resolution of one of the major problems of cryptography – the problem of key distribution. At the same time researchers face new serious problems. One of major problems is speed of encryption and decryption algorithms. Such algorithms are slow. Namely they are considerably slower than algorithms of symmetric cryptology. The difference in the processing speed is so considerable that it forces to refuse direct application of asymmetric algorithms for encryption information. It is instead limited to the asymmetric encryption of the secret key of symmetric cryptosystem. Fast symmetric algorithm is used further in the session of encryption.

Taking importance of speed problem of asymmetric cryptosystems into account, a number of researchers distinguish research and development of computational algorithms into independent direction of asymmetric cryptology [3]. Results that have been given in this article concern exactly mentioned above direction.

Thus, as it was already said, the problem of asymmetric algorithms of encryption is their low processing speed. That is why researchers try to improve this processing speed. Summing up these attempts it is necessary to establish the following. Absolute majority of these attempts will be realized within the limits of algorithmic principle of calculations. Thus computational algorithm is built as complete sequence of operations on numbers: values of arguments, constants, etc.

At the same time there is analytical principle of calculations. The work of analog machines was based on this principle. Realizing this principle, a model of a calculable transformer is built. The model is similar to a transformer. And the concept of similarity is certain. After the model is created it is assigned some initial values including the argument. Then the model processes the necessary increase of argument forming the proper increase of function.

Usually, it is difficult to find application of the analog transformers of this type in asymmetric cryptology. For these transformers considerable errors are typical that are impermissible for calculations in the complete numeric fields. But there are the digital devices, which work on analytical principle of calculations. They are also called digital analogues or pulse-number functional converters. At one time such devices were forced out by universal algorithmic computing facilities. Today their application domain is limited mainly to measuring devices, computer graphics and some specialized calculators. However due to reduction of prices of the specialized computing facilities the application domain of digital analogues extends again.

Digital analogues are a compromise between speed of analog computing facilities and accuracy of digital algorithmic computing facilities. In applications such as functional signal processing of frequency transducers or pulse-number codes (which are used in particular in measurements of unknown value by reference one), during the functions tabulation and in other applications, where an argument is decomposed into sequence of increases, digital analogues taking speed into account concede only to the tabular functional transformers. If one can select functions tabulation from the mentioned applications, then in the context of instability of asymmetric cryptosystem to the attack with the chosen plaintext we should notice the following. The brute force attack with the chosen plaintext in that or other asymmetric cryptosystem can be interpreted as tabulation of that or other one-way function. Thus, digital analogue is one of the fastest digital facilities of realization of such attack. But is it possible to build a digital analogue for the design of one-way function? In fact Shannon in his well known theorem [4] talked about possibility of recreation of continuous functions. In addition, digital analogues have calculations errors, considerably larger from rounding errors. During the calculation of majority of one-way functions, where module reduction is computed, errors are inadmissible. All these problems concern creation of digital analogues for the recreation of one-way functions. The ways of solution some of them are offered in this article. There is also another problem – is there a place for digital analogues in asymmetric facilities of encryption-decryption or not. In fact in the process of encryption-decryption an argument is not similar to the sequence of identical increases unfolded in time, with which a digital analogue can function. This problem is also considered in this article.

2. FUNDAMENTALS OF DIGITAL ANALOGUES SYNTHESIS

The basic structural element of digital analogues is a device called digital integrator, digital differential analyzer or pulse-number multiplier. Several other terms are known also.

The simplified structure of such a device, adapted to treatment of single increases of arguments [5], is presented on Figure 1.

The device consists of a counter **CT** of the increases of a sub-integral function and accumulating adder. It consists of combination adder **SM** and register **RG**. The device realizes the method of rectangles for marked integral calculation. As soon as the next single increase of the integration variable **X** is formed at the input **ΔX**, the increase of the **Y** integral is added to the previous value of the integral accumulated in the register **RG**.

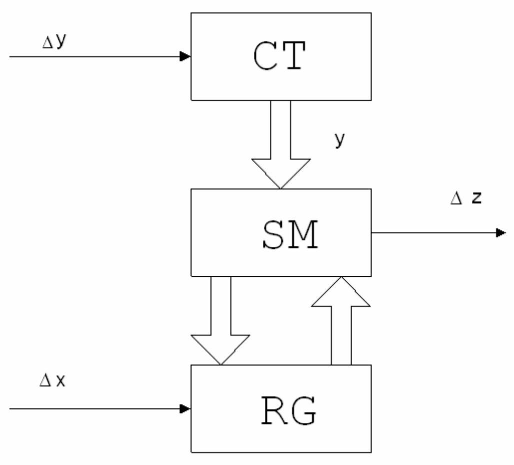

Fig.1 – Digital integrator structure chart based on adder accumulator.

As soon as the accumulated integral value exceeds the capacity of the **Nm** register, a single increase of the integral will be formed at the output of adder **SM**. That is why approximately we have the following equation of structure operation:

$$\Delta Z = \frac{y}{N_m} \Delta x$$

It approximately corresponds to differential equation:

$$dZ = \frac{y}{N_m} dx$$

But only approximately, because we have the integration error and rounding error.

Except for the digital integrator it is necessary to have adder of increases. These two types of structural elements, after well-known Shannon's theorem, are sufficient to reproduce any continuous function.

For example, if we need to reproduce a function:

$$z = \frac{1}{x},$$

we differentiate it to get generating differential equation:

$$dz = -\frac{1}{x^2} \cdot dx$$

Then we can always decompose this equation into a system, which, according to Shannon’s theorem, contains only operations of integration and summing up. For example, such a system:

$$\begin{cases} d\alpha = \dfrac{z}{N_m} \cdot dx \\ dz = -\dfrac{z}{N_m} \cdot d\alpha \end{cases}$$

It is possible also to get other systems if we have a wider set of structural elements:

$$\begin{cases} d\alpha = \dfrac{x}{N_m} \cdot dx \\ dz = -\dfrac{N_m}{\alpha} \cdot dx \end{cases} \qquad \begin{cases} d\alpha = \dfrac{z}{N_m} \cdot dx \\ dz = -\dfrac{N_m}{x} \cdot d\alpha \end{cases}$$

$$\begin{cases} d\alpha = \dfrac{N_m}{x} \cdot dx \\ dz = -\dfrac{N_m}{x} \cdot d\alpha \end{cases} \qquad \begin{cases} d\alpha = \dfrac{N_m}{x} \cdot dx \\ dz = -\dfrac{z}{N_m} \cdot d\alpha \end{cases}$$

However, we will get back to asymmetric cryptology.

3. THE DIGITAL ANALOGUE SYNTHESIS FOR THE RECREATION OF RABIN'S ONE-WAY FUNCTION

Rabin's asymmetric system is based on the following one-way function [6]:

$$\text{SQUARE}(x, k) = \left\langle x^2 \bmod k, k \right\rangle$$

The same function, in accordance with the binary algorithm of raising to the power, we constantly calculate in the RSA system. It is a parabola in the complete numeric field - such a "chopped" parabola (Figure 2).

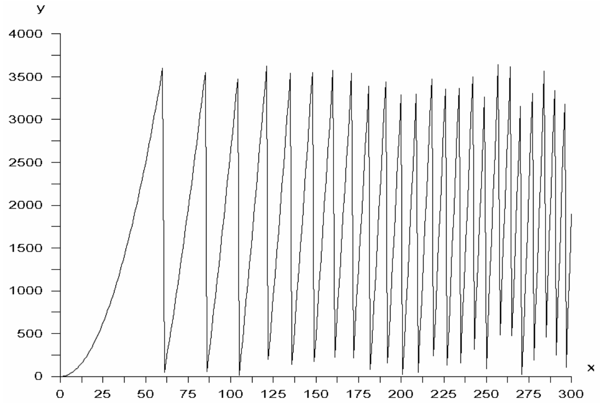

Fig.2 – Parabola in a numeric field

First we will consider a model (digital analogue) for the calculation of function $y = x^2$. We differentiate this equation. And we get generating differential equation:

$$dy = 2xdx$$

Only one digital integrator with the following links can be the model of such ideal transformer (Figure 3):

Such transformer (Figure 3) works in accordance with such difference equation:

$$\Delta y = \frac{x}{2^n} \Delta x$$

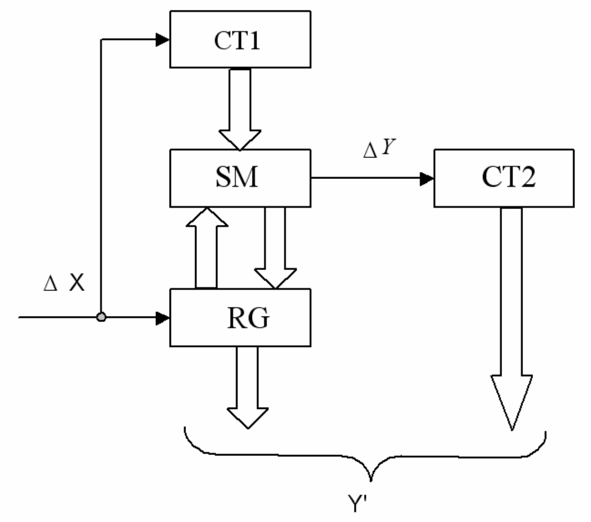

Fig.3 – Digital analogue for the approximate calculation of function

Or in accordance with such equation, if the number in the register is read as less significant digits:

$$\Delta y = x \cdot \Delta x$$

This equation within the error of integration corresponds to such differential equation:

$$dy = x \cdot dx$$

We integrate it:

$$y - y_0 = \frac{x^2}{2} - \frac{x_0^2}{2}$$

We will get such equation:

$$y = \frac{x^2}{2},$$

with such initial conditions:

$$y_0 = \frac{x_0^2}{2}$$

Consequently, we obtained a result proportional to the necessary one. However we obtained it with an error of integration. But for the calculation of function X^2 a well-known method which allows avoiding the error of integration can be applied. Let us assume that at some i-step of model operation we have the following i-result:

$$y_i = x_i^2$$

Then, we increment the argument and receive the following result:

$$y_{i+1} = x_{i+1}^2 = (x_i + 1)^2 = x_i^2 + 2x_i + 1$$

Thus in the considered structure (Figure 3) we need code **X**, accumulated in counter **CT1**, to pass to adder **SM** with 1 digit shift. Thus we will realize multiplication **Xi** by two. And "one" is passed to the less significant digit of adder (Figure 4).

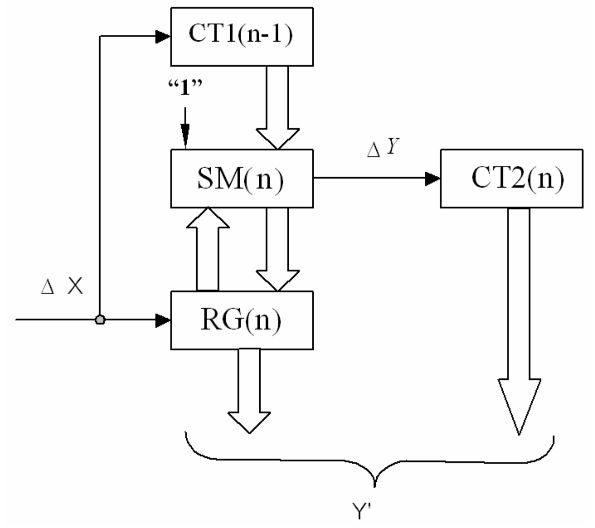

Fig.4 – Digital analogue for the exact calculation of function

This is enough to remove the error of integration.

Now, if the result is read from counter **CT2** it is determined as follows:

$$y = x^2 \bmod 2^n$$

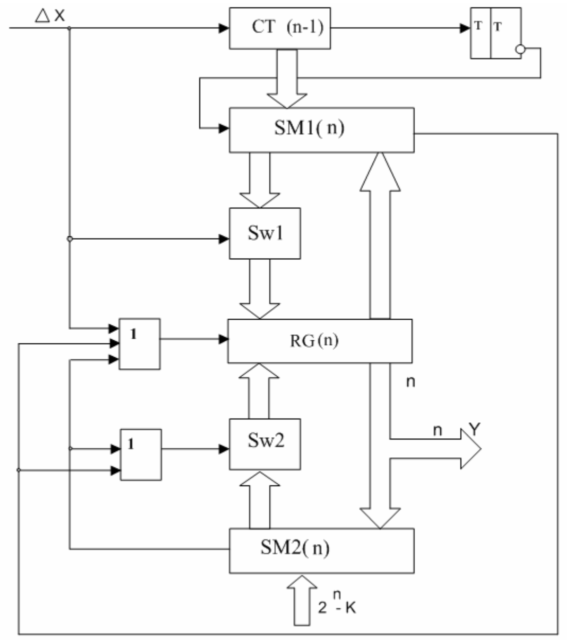

Fig.5 – Digital analogue for the calculation of Rabin's function

But, we must conduct the calculation by module **K**. That is why we complement the structure with another accumulating adder (Figure 5) which compares an intermediate result to the module of **K** and if necessary decreases a result by module **K**. We also use measures for sub-integral function range expansion (trigger on a Figure 5). As a result we get the digital integrating model of reproducer of Rabin's function.

Let us assume that we apply such model for the realization of a brute force attack with the chosen plaintext against Rabin's system. If we modify the value of argument by "one" ($\Delta x = 1$) in such model, we will get new result during a time period that approximately equals to the actuation time of two multi-bit adders – SM1 and SM2 (Figure 5). I.e., the maximal frequency of calculation of possible decisions by such model is approximately the following:

$$f_{\max} \approx \frac{1}{2 \cdot t_{SM(n)}},$$

where $t_{SM(n)}$ is the actuation time of n – bit adder. Thus we carry out only two additions for the search of every new decision. If we build SM1, SM2 using classical structures of adders with the sequential, parallel or combined carry, the frequency of calculation will depend on the precision of the model. The time $t_{SM(n)}$ will be considerable too. But we can build the structure elements on Figure 5 using the conveyor structures which are offered in [7]. The adder of such structures is built as bit-by-bit conveyor. Processing by the different digits of adder of the same increase is divided in time. The least significant bits of adder, which have finished processing of previous increases, process the following increases. At the same time the higher digits continue processing of previous increases. The processing frequency of argument increases in such structure depends only on actuation time of one-bit adder (least significant bit), that is approximately in two times less than maximal operation frequency f_0 of the chosen element base [7]:

$$f_{\max} \approx \frac{1}{2} f_0$$

The time period of calculation of full digit conversion result is increased however in a conveyor structure. But this time period is fixed and does not influence on the fact of model operation in real time.

Thus, the considered model calculates the value of Rabin's function for the sequence of neighbouring values of arguments actually with maximum frequency of the chosen element base. Parallel application of several models allows increasing this frequency by the corresponding number of times. That is why such model can be interesting in cryptanalysis for brute force attack with chosen plaintext. If we speak about encryption, then direct application of this model is not advisable for the real key length. We will pay attention to the prospects of application of one-way functions digital analogues in encryption in the following material.

3. THE PROBLEMS OF CONSTRUCTION OF DIGITAL ANALOGUES OF ONE-WAY FUNCTIONS

Thus, we succeed to avoid the integration error in modeling of Rabin's function. For this we applied the principles of synthesis that differ from the classical Shannon's principles. The exact digital analogues of the majority of other one-way functions cannot be synthesized using the classical Shannon's principles too. The exact digital analogues of some auxiliary of functions, important in the process of the asymmetric encryption, can be synthesized using a classic method, for example, the function of multiplication of variable by a constant or the function of multiplying of two variables. The recreation of power functions (for small powers), applying such an approach, similar to that which we considered on the example of Rabin's function, is possible without the calculation error. And such functions are in the basis of many asymmetric cryptosystems. Thus the digital analogues of power functions should be built depending on exact expression for the function increase. And this expression contains all power functions with lower powers. E.g., let us consider equation, which can be used for the synthesis of integrating models of function $y = x^4$ (the increase of function is underlined):

$$y_{i+1} = (x_i + 1)^4 = x_i^4 + \underbrace{4x_i^3 + 6x_i^2 + 4x_i + 1}_{}$$

It results in considerable complication of transformer structure. That is why for large power values, the practical realization of such models is problematic. At the same time for small power values (i.e., for RSA it is recommended by some standards - 3, 17 or even 65537) the construction of power digital analogue is entirely possible. And the operation frequency of such model will be two times less than operation frequency of Rabin's function conveyor model (additional cycle is needed for adding up the partial increases formed by the lower power transformers). At the same time the construction features of power digital analogues exceed the bounds of introductory positions of this article and are the topic of separate consideration.

In case if construction of the exact digital analogue of one-way function is not succeeded, it is possible to try one of the next variants. The first one - realization of the model with an error, requires consideration of several possible solutions and choosing the only correct (if there is the criterion of such choice). The second variant is the realization of the compound model. The example of the second variant can be the model of reproducer of exponential one-way function (Figure 6).

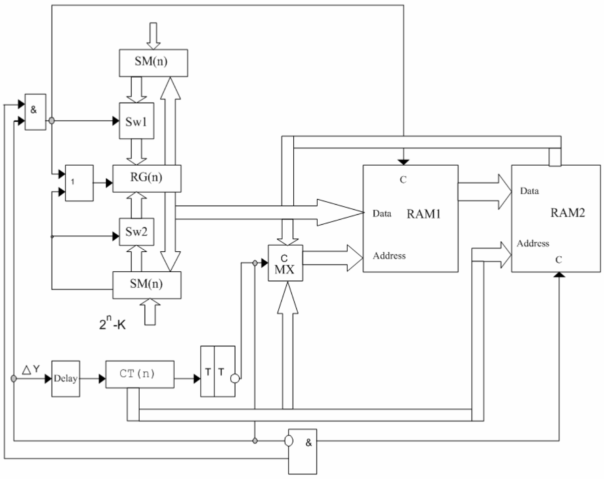

Fig.6 – The model of reproducer of exponential one-way function

It is known that to get the new value of exponential function increasing its argument by "one", it is sufficient to multiply the previous function value by primitive root by module K. It is also known that changing of value of argument **X** from 0 to (K-2) with step 1, the exponential function takes all integer values from this range:

$$1 \le y \le K - 1$$

And it means that in the process of calculation of exponential function for all **X** from the specified finite numeric field, all integer values from this field should be multiplied by a primitive root by a specified module. That is why the basis of exponential transformer model is digital integrator of constant – primitive root of **q** (Figure 6). The second part of the model is a two memory devices. At the first stage of the model operation, the digital integrator works and all products of integer values by primitive root of **q** is written down in **RAM1**. At the second stage of the model operation a kind of "shuffling" the results obtained at the first stage is carried out by **RAM1** and **RAM2**. These results take place in the necessary order. Unfortunately, this model is considerably slower than the model of Rabin's function.

Thus, we considered the examples of integrating models of one-way functions. It was already said about the possibility of direct application of these models in cryptanalysis. But is there a place for such models in asymmetric cryptography? In fact the models work with unitary increases. And in asymmetric cryptography we operate with large numbers.

4. PROBLEMS AND PROSPECTS OF DIGITAL ANALOGUES APPLICATION IN ASYMMETRIC ENCRYPTION.

Let us consider the problem of digital analogues application for asymmetric encryption. Suppose that we have the result y_i of calculation of some one-way function from some argument (or block) of x_i. In order to get the result for the next block x_{i+1}, we must find the following difference:

$$\Delta x = x_{i+1} - x_i$$

After that we need to decompose this difference into a sequence of unitary increases, then run this sequence through the model and obtain a result. If the values of arguments are large this means that the difference is probably large too. And that is why the sequence of unitary increases is very long and the operation time of model is impermissibly long.

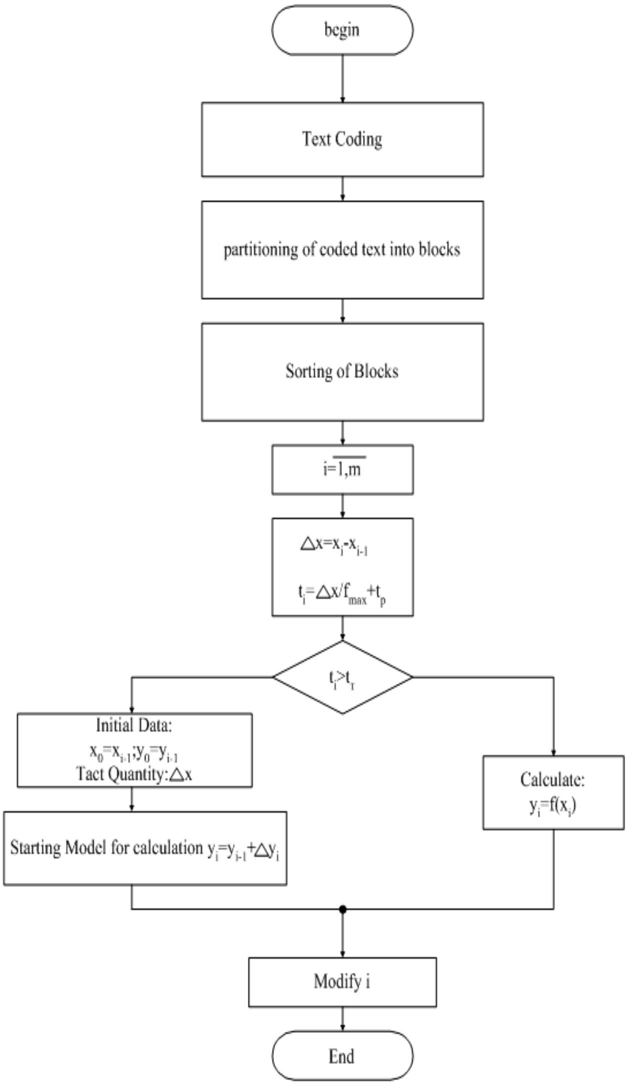

Fig.7 – The algorithm of the choice of efficient calculation method

Thus, everything depends on the size of differences between the blocks of information, which comes for crypto-operation. On the Figure 7 there has been shown the algorithm of the choice of efficient calculation method. If the difference is bigger than some threshold value – we choose an algorithmic method. If smaller – we start a model and realize the analytical method of calculation. But what is the fate of small differences and how often the analytical method of calculation will be involved?

The importance of this question points out the necessity of researching the distribution of differences. Such research has been conducted, for different texts - English, Ukrainian, Russian, for files of different type, for different block lengths (Figure 8).

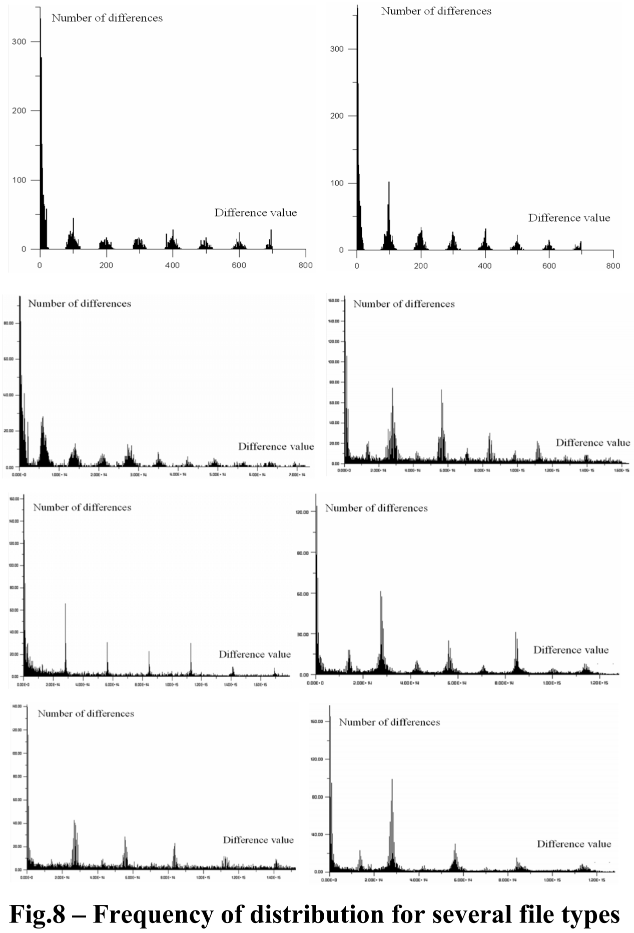

Fig.8 – Frequency of distribution for several file types

The character of such distribution is invariable on the whole and depends neither on language nor from a file format. Even compressed files, which have hidden statistical language features, keep the features of distribution of differences between blocks. What are these features? First of all, the amount of differences diminishes with growth of their size (Figure8). It is clear as a small difference can show up both between the small values of argument and between large. And a wide difference can be only between the large values of argument. The second feature of distributions is the periodic growth of amount of differences. The reason for this is the frequency irregularity of fragments of information. That means that there are more used fragments of information - combinations of letters, combinations of words, language idioms; frequently used fragments of code in files. During the distribution of information into blocks these frequently used fragments get into different blocks with different shifts. That is what causes periodic growth of amount of differences. The period of this growth, as a rule, is the maximum capacity of the alphabet used for information coding.

The character of differences distribution lead to the idea of combined method of one-way function calculation. In fact a difference can be divided into two increases of the second order. The first part of the increase is greater – it will be divisible to the period of distribution. It can be processed by an algorithmic or tabular method. The second part of the increase – the smaller one – is possible to process with an analytical method using the digital integrating model of functional transformer. For example, we perform encryption using the Rabin's method and we get the result of encryption y_1 of the plaintext block x_1. It is thus known that every plaintext character is encoded by a byte. Then we can present the following plaintext block in this way:

$$x_2 = x_1 + s \cdot 256 + \Delta_2 x$$

Consequently from nature of differences distribution we get that $\Delta_2 x$ often appears a small number. The next ciphertext block is determined in the following manner (module reduction is omitted):

$$y_2 = x_2{}^2 = (x_1 + s \cdot 256 + \Delta_2 x)^2 =$$
$$= y_1 + s^2 \cdot 256^2 + 2s \cdot 256 \cdot x_1 + 2x_1 \cdot \Delta_2 x + 2 \cdot \Delta_1 x \cdot \Delta_2 x + \Delta_2 x^2$$

In this expression y_1 is previous ciphertext block. A tabular transformer can calculate the next item. The third item can be calculated by an incremental linear digital analogue (this is a structure, which processes not single increases, but increases that are equal to integer powers of 2). In such transformer x_1 is a coefficient, and a number $2s \cdot 256$ is decomposed to the sequence s of input increases of integration variable. Three last items can be calculated by digital analogues. First and second items from mentioned above three are calculated by linear digital analogues (bigger multipliers $2x_1$ and $2\Delta_1 x$ are the increase coefficients, and a small number $\Delta_2 x$ is decomposed into the sequence of single increases and is the integration variable). The last item is calculated by the digital analogue of Rabin's function.

5. CONCLUSION

Finally, summing up everything that has been said, the following can be established. Developed digital integrating models in fact reproduce one-way functions. In a number of applications they provide considerably higher processing speed than algorithmic methods of calculations. Based on the obtained results, it is possible to offer the following perspective directions of further research.

1. Development and research of digital integrating models of one-way functions with the ternary coding of information.
2. Development and research of incremental reproducers of one-way functions.
3. Research of distributions of differences and development of the combined calculators of one-way functions. Namely those that combine algorithmic methods of functional processing of the larger part of the increase and analytical processing methods of the smaller part of the increase.

6. REFERENCES

[1]. W.Diffie and M.E.Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, v. IT-22, n.6, Nov 1976, pp.644-654.

[2]. R.C.Merkle, "Secure Communication Over Insecure Channels", Communication of the ACM, v. 21, n.4, 1978, pp.294-299.

[3]. A.V.Lunin, A.A.Salnikov "The prospects of development and application of assymmetric cryptography algorithms". Confident, №10 – 1999.

[4]. Maksymovych V., Dudykevych V., Gorpeniuk A. "New hardware for pulse fluxes processing", Proceedings of the X Polish national conference "Application of microprocessors in automatic control and measurements", v.2.- Warsaw, Poland, 1996.- p.150-157.

[5]. Maksymovych V., Dudykevych V., Horpenyuk A., "New hardware for pulse fluxes processing", Application of microprocessors in automatic control and measurements: Proceedings of the X of Polish National conference. Warsaw, Poland, 1996.- p.150-157.

[6]. M.O.Rabin, "Digital Signatures and Public-Key

Functions as Intractable as Factorization", MIT Laboratory for Computer Science, Technical Report MIT/LCS/TR-212, Jan 1979.

[7]. Andriy Horpenyuk "Reversible pulse-numerical functional converters",- Manuscript. Thesis for a Ph.D. science degree in speciality 05.13.05 - elements and units of computer technique and control systems. - State University "Lvivska Polytechnica", Lviv, 1998.

Andriy Horpenyuk
Graduated from Lviv Polytechnic Institute in 1993 on the speciality "Automation and Telemechanics". In 1994 has defended the master of technical sciences degree on the subject "Pulse-numerical converters of frequency-time signals". In 1998 has defended a candidate thesis on the subject "Reversible pulse-numerical functional converters" and received PhD degree. In 2002 has got academic status of associate professor. Author of 30 scientific articles. Areas of interests: pulse-numerical functional converters, pulse-numerical measuring converters, technical information security, cryptology, computational cryptology algorithms.