Failure consequences imitation modelling in the equipment of data protection and datastorage systems

Urbanovich P.P.[1, 2], Halaburda A.I.[2], Romanenko D.M.[2], Makas S.B.[2]
[1] *Katholic University of Lublin, Poland, E-mail: Upp@rambler.ru*
[2] *Belarusian State Technological University, E-mail: Sergey_X@lycos.ru*

Abstract: *An effective and easily realizable method of failure consequences detection in units of the device realizing block cryptoalhoritm GOST 21147-89 of the information protection is submitted and also the imitation model of a protective system and data storage has been designed.*

Key words: Fault-tolerance, block cipher, imitational model.

1. Introduction

The problem of information protection and its transfer channels from unauthorized access is becoming more and more vital. Cryptography methods are considered to be ones of the most reliable.

For the information transmitted through high-velocity communication channels to be confident, it is necessary to find the algorithm, which ensures the conversion in the real-time mode. Modular cryptoalhoritm GOST meets these requirements.

The aim of this research is the analysis of the error-spread effect in the device realizing the given algorithm. The research is carried out on the basis of imitative and statistical modeling.

The elements of arithmetical logic and data storage will be generally used in a converter unit of the information. The semiconducting memory elements and registers are related to the elements of data storage, where operative information of cryptoconversion process is stored. It is evident, that the elements of arithmetical logic are those with the small integration scale (unlike the elements of memory). Therefore it is important to investigate the problem of memory operational reliability as a basic device component and to determine the degree of memory malfunction influencing the process of the error-spread effect by a converter unit of information.

2. Object model of the cryptoconversion device

Let's consider features of the device realizing algorithm GOST.

The algorithm under analysis is a modular one. This means that the data for encoding are divided into units of 64 bits, each one is further subjected to repeated transformations. The number of elementary conversions is 32. The device consists of two storage devices, summation modulo 2^{32}, and unit of key information storage, unit of substitution, summator modulo 2 and shift register.

While designing the program the authors have proceeded from the following limitations: there aren't group errors, only a single error on the time period between receiving the data on encoding and obtaining the outcome is possible, the probability density of an error (intensity of errors) is constant, and does not depend on time, the error is considered to be inverting of the bit value.

The base model of the program is a simplified diagram of the device described above. The principle of the programming model operation of failure consequence research consists in quantifying the distinct bits of a data word in a data block, converted by the algorithm without an error, and in the unit obtained as a result of the algorithm allowing for errors.

As the model of the simplified device scheme is realized using the object-oriented programming concepts, we shall consider the diagram of classes and its realizing (Pic.1).

The main activity is performed by the object of the Crypto class. This class encapsulates methods modeling the information converter unit. This class represents the container with the lists of classes - components, realizing separate clusters of the modeled device. Classes - components: *Sum32* - unit of summation modulo 32, *Sum2* - unit of summation modulo 2, *Substitution* - unit of substitution, *Shift* - unit of a circular shift on 11 bits.

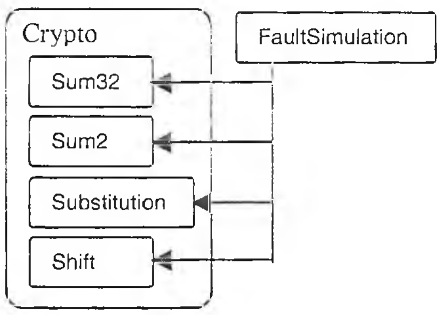

Fig.1

We shall consider the *FaultSymulation* class separately. This class encapsulates methods and properties for imitation the flow of errors and malfunctions, which can arise in elements of the conversing device. The imitation of errors originating process implements according to three principles of statistical modeling: 1) processes of imitation consist of three stages: modeling the error type (malfunction or failure in a certain element of the hardware), error address (certain element of the given type) and time of malfunction or failure; 2) in a certain point of time no more than one event can take place; 3) the errors and failures flow, which is characteristic for the term of accidental errors, is modeled, when the failure rate of the device is constant and does not depend on time ($\lambda_{Ycm} = const$). The class of the flow error flow modeling with given distribution operates with a following data set: 1) information on the quantity of element types of the conversing device; 2) intensity of malfunctions or failures for a certain type of members; 3) quantities of elements of one type; 4) values of parameters of elements; 5) information on certain group of events for the given model.

3. Failures modeling

The main event is the total failure of the device. The given event has certain intensity which is failure rate of the device λ_{Ycm}. This value is added from the total failure rate of all elements of the conversing device $\lambda_1 + \lambda_2 + .. + \lambda_n = \lambda_{Ycm}$, where n is the number of element types of the device. Proceeding from this, the first stage of errors modeling consists in type selection of an error element, which will be implemented with intensity, proportional value of malfunctions (failures) intensity of this type units. The value modeling process of the error distribution by the types is subject to the distribution of infrequent events of the Puasson. The modeling algorithm of infrequent events is the following: a variable (0,1) is divided into n parts (n - quantity of errors types), where each i part is equal $\lambda_{\sum i}$, where $i \in [0, n]$, $\lambda_{\sum i}$ - general relative rate of device elements failure of i type. The hit of a random value in i variable is fixed as event A_i. The number of hits m_i in i segment is proportional to its length, i.e. the relation of the hits number of a random value on i variable to the general number of tests M is received as a probability of the event occurrence A_i, $P(A_i) = \frac{m_i}{M}$. The probability $P(A_i)$ is considered to be constant on all the variable. Thus we receive, that the event A_i (modeling of an error of i type) is replicated with frequency, which is proportional to its probability. At application of the algorithm on a computer, the problem is reduced to check the uniformly distributed random value $\varepsilon_i \in [0,1)$ According to the inequality: $\sum_{i=0}^{k-1} P_i < \varepsilon_i \le \sum_{i=0}^{k} P_i$, where $k \in [0, n]$ and the value k, at which this equality will be true, will give the number of the disruptive element of the cryptoconversion device.

The number of the disruptive element of i type, the address of error z_i, is modeled by the uniformly distributed random value varying from 1 to n_{z_i}, where n_{z_i} is the number of elements of i type. The given value is calculated by conversion of the variable of the uniformly distributed random value ε_i. If n_{z_i} is accepted as a bound on a variable, the expression for obtaining number of the failed element of a i type has the form: $z_i = 1 + (n_{z_i} - 1) \cdot \varepsilon_i$ [1].

The random moment of malfunction (failure) of elements t_i is modeled by exponential law of distribution with mathematical expectation $M(t_0) = \frac{1}{\lambda_{Ycm}}$, - where λ_{Ycm} is general rate of cryptoconversion device failure.

Complexity of the device and the specific units activity of the modeled device lead to the necessity of registered event accurate definition: in what parameter what event, which is specific for the given element, has happened. To solve this problem it is most convenient to present events' structure by the tree-type list. Here all events are divided into the groups (clusters), which are specific for certain elements of the considered device. Each group represents the unit, which can represent as the root of a cluster branch of events, which are specific for the given group.

Applying the tree structure of error distribution by the types, the algorithm of the event reproduction is the following: the modeling starts with the selection of a unit in the tree root. Having obtained the number of a unit (group of faults), the unit with the obtained number is examined in order to find any own events' branch, for which it will represent the general intensity of faults. The process of descending the tree will be repeated until the unit without a branch of events will be retrieved. If the obtained unit has not a branch of events, the event, which is determined by this unit, is registered.

In the primitive case, when the tree of events grouping is double-leveled, the following equality should be true for any relative intensity of all events:

$$\sum_{i=1}^{n}(\lambda_i\cdot\lambda_{i1}+\lambda_i\cdot\lambda_{i2}+\lambda_i\cdot\lambda_{ij}+..+\lambda_i\cdot\lambda_{im_i}) = \sum_{i=1}^{n}\left(\lambda_i\cdot\sum_{j=1}^{m_i}\lambda_{ij}\right)=1.$$

Where n - quantity of events groups (quantity of clusters in the tree root), $i\in[1..n]$ - quantity of clusters in the root tree, λ_i - intensity of i group of events, λ_{ij} - intensity of event $j\in[1..m_i]$ in i group, m_i - quantity of events in i group.

The representation of the whole group of events by the tree-type list, grouped by the types of the modeled device elements represents a convenient way of classification and detailed calculation of events after the termination of the modeling process.

The sequence of operations in the program is the following: the user sets a number of tests, and selects a mode of research, and also the unit, which is subjected to research. Then the random mode generates the unit of input dates key, there are two cryptoconversion's objects, one of them is initiated by the object with the uniformly distributed cumulative distribution function of the probability density, and the second is the object, which does not generate errors. Than there is encoding of a data block through these objects and the result of the program is the injected quantity of the distinct bit in outcomes.

4. Conclusion

The given research has offered a new approach to the creation of the research failures consequences computer model of different units of the cryptoconversion device. The offered new technique combines in itself methods of imitative and statistical modeling.

As a result of the program the data are obtained, which permit to affirm that already after the eighth iteration the quantity of error bits in a data word exceeds 32, which is a parameter of the full loss of self-descriptiveness of information.

Bibliography

[1] Урбанович П.П., Алексеев В.Ф., Верниковский Е.А., Избыточность в полупроводниковых интегральных микросхемах памяти. – Мн.: Навука і тэхніка, 1995.

[2] Домашев А.В., Попов В.О., Правиков Д.И. Программирование алгоритмов защиты информации. – М: Нолидж, 2000. – 288с.

[3] Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб.: Лань, 2001. – 224с.