ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 2, February 2019

The Synthesis of the Control Unit for Implementation Of Algorithms Cryptography (AES).

Anvar Kabulov, Sherzod Boltaev, Alisher Dusmukhamedov

Professor, Dept. of Information Security, Faculty of Mathematics, National University of Uzbekistan named after Mirzo Ulugbek & City Tashkent, Uzbekistan.
PhD Researcher, Dept. of Information Security, Faculty of Mathematics, National University of Uzbekistan named after Mirzo Ulugbek & City Tashkent, Uzbekistan
Researcher, Head of the Department of Information Security, State Customs Committee of the Republic of Uzbekistan & City Tashkent, Uzbekistan.

ABSTRACT: - The article deals with the synthesis of automata for the implementation of the control operation, the model of the information security system constructed using the algorithmic automata approach is presented. Introduces the concept of a monitor - a special unit that performs a control operation in aggregate systems, designed to control the aggregates of this system. A technique for algorithmizing the design of embedded control systems and information security based on distributed microprocessor systems on matrix LSIs is proposed.

KEYWORDS: Algorithmization, design, management of system, Information Security, matrix BIS, system of microprocessor , abstract automation, model of system, logic, modeling.

I.INTRODUCTION

The aim of the article is to develop logical control and information security systems based on programmable microcontrollers for managing and actively protecting informatization objects and ensuring the security of information circulating in organizations and departments. The objectives of the article are the construction of control monitors based on finite automata and the implementation of cryptography algorithms, methods and means of technical protection of information based on programmable microcontrollers.

Standard description of complex systems. The problem of the standard description of systems is given in / 1-2 /, where the authors proposed a universal automated model of complex systems, described with the help of aggregates and aggregate systems.

These models are called aggregate, and aggregates are represented in the form shown in Fig. 1.

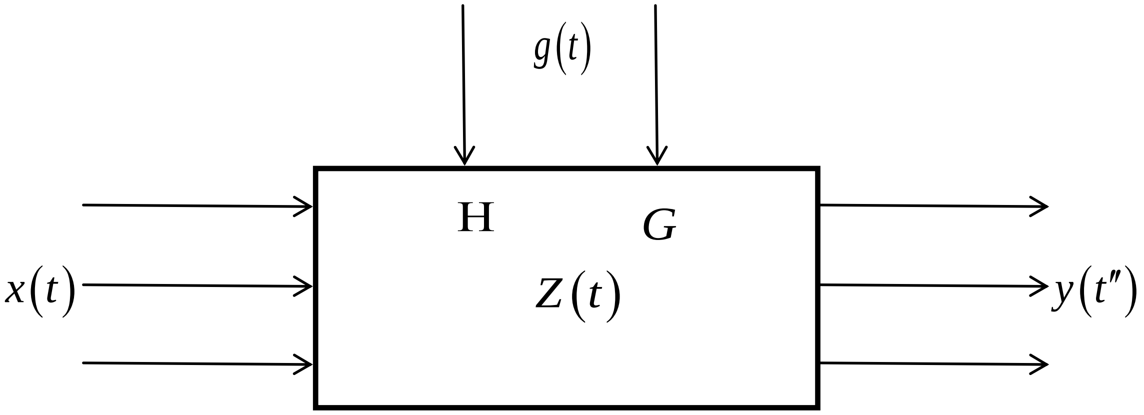


Fig. 1 Models of aggregate.

In principle

$$Z(t) = H[Z(t_0), t]$$

The operator is deciphered as follows. When the input or control signals arrive and the output signal is output, the unit is in a special state, from which it jumps to a new state.
Here 4 cases are possible: filed -, and issued:

$$\begin{cases} Z(t^{*}+O)=V^{'}[Z(t^{*}),\ x,\ g_{s}] \\ Z(t^{*}+O)=V^{''}[Z(t^{*}),\ g] \\ Z(t^{*}+O)=V[Z(t^{*}),\ x,\ g] \\ Z(t^{*}+O)=W[Z(t^{*}),\ g_{s}] \end{cases},$$

where is the last to control signal. In the intervals between special states we have:
The operator consists of two parts: -produces the output signal, -assesses belonging to the subset.
It is assumed that the state of the unit changes abruptly. In the terminology of the TF, the operator corresponds to the operations, and Z is the aggregate of the states of the aggregate A. It is assumed that in each clock cycle, the state of the corresponding aggregate Z varies with respect to (I) in the unit of signals of the X, y, (X, y) type; output signals (y), (U), (y, U) are possible.
Consider complex systems using graphs, for which the following characteristics exist: coordinates, time intervals, operations and states. We call such an element the workplace (PM) and we will designate it as follows: where is the coordinate vector in the -th time interval - the set of coordinates PM;
-jth time interval (T - set of time intervals);
- the operation performed in the -th time interval (D is the set of operations);
is the state vector of the ith PM in the time interval (P is the set of PM states).
The set of PMs connected by attributes is determined by some network in each time interval [3]. Changes in the PM network in time - a function of changing the network F (t). Such a description of the system will be called the table of functioning (TF) of the system. Graphically, each operation - performed on the PM at a time has coordinates
The time intervals during which the TF structure remains unchanged will be called technological cycles. In the terminology of the TF, the operator corresponds to operations, and Z is the aggregate of states of aggregate A. In this case, a separate unit corresponds to one PM and one TF operation, and the aggregate system (A-system) as a whole corresponds to an individual technological cycle of TF. In production systems described by A-systems, in all formal approaches use the operations of assembly, processing and management. In this case, there are several forms of recording the performance of aggregates of these operations, convenient for implementation on a computer; for example, operator schemes (OS).
In discrete manufacturing, when describing the operation of processing, assembly and control, combined OSs are obtained. But the principle of their construction remains unified. In the process of combining the above-mentioned aggregates an aggregate system is created. The functioning tables introduced in / 3-4 / and formally defined in this paper have, in our view, a logical continuation and development of the definitions of aggregate systems and allow us to use the best aspects of formal apparatus for describing manufacturing systems for solving the problem of algorithmization of control.

II METHODOLOGY

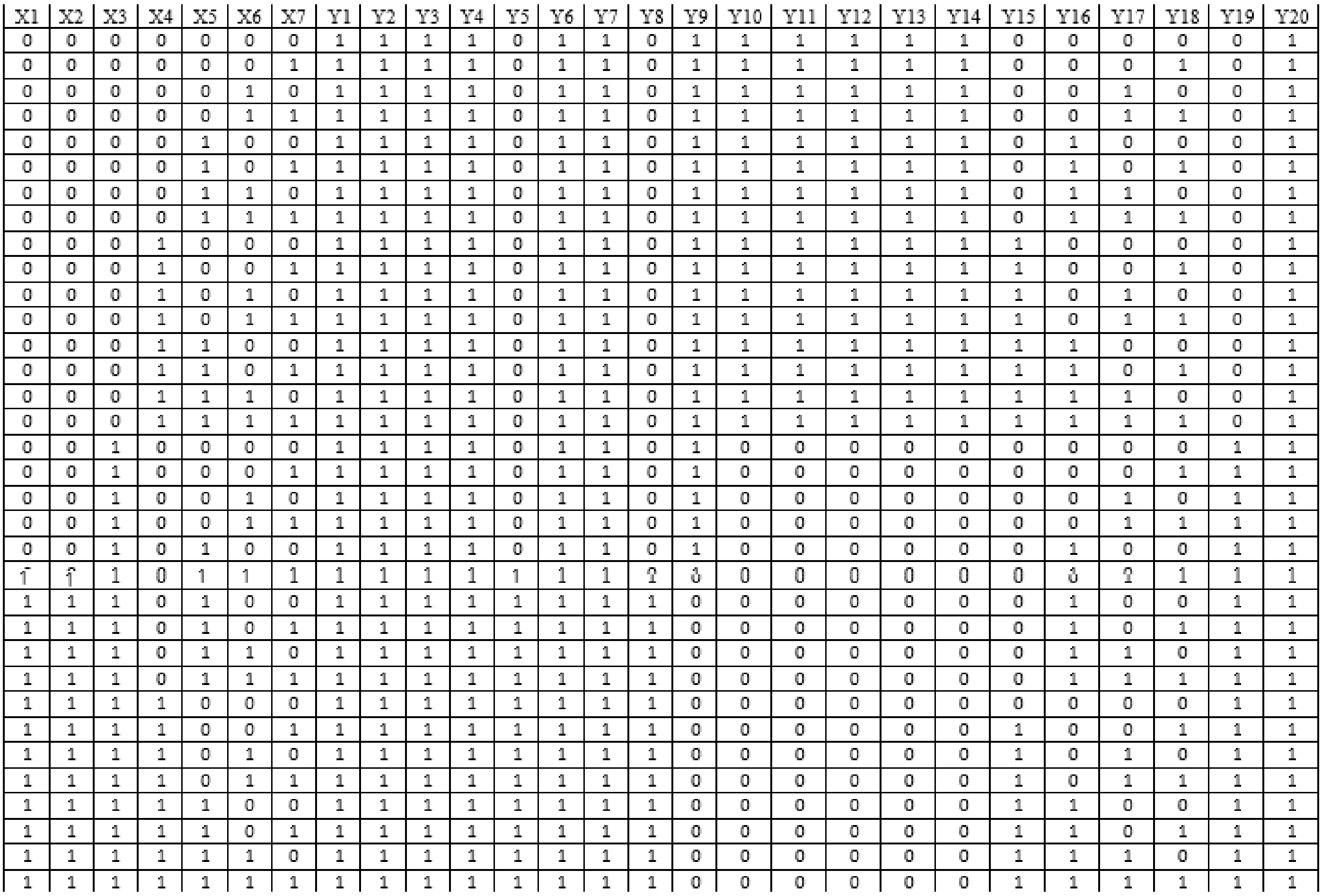
THE TASK OF SYNTHESIZING THE CONTROL UNIT (MONITOR).

Consider the process of synthesizing automata for the implementation of a control operation. We introduce the notion of a monitor-a special aggregate that performs a control operation in A-systems. A monitor is an aggregate or complex of an A-system designed to control the aggregates of this system. The monitor is responsible for the distribution of the relevant input information for the system units, and also controls the operation of the units. For example, in operating systems, there may be a main memory monitor and a CPU monitor, and in the machining systems there are monitors for local management of a group of CNC / 5 / etc. machines.
The monitor is given the right to access information tables and other managing structures of the A-system associated with the control unit.
A universal monitor we call a monitor, which consists of a control unit that receives as input information a set of instructions for execution. A model of a universal monitor of an A-system can be a finite state machine with a memory memory / 6-7 /. To obtain a finite alphabet of store symbols, we use the technique of synthesizing control automata

according to GAW / 8 /. According to / 6-8 /, the technique consists of two stages. The first step is to mark up the GAW with symbols (labels) using the following algorithm:
Step I. The symbol marks the input of the vertex, which follows the initial one, and the output of the final vertex.
Step 2. The inputs of all vertices following the operator are marked with symbols.
Step 3. Inputs of different vertices, with the exception of the end, are marked with different symbols.
At the first stage e we get a marked GAW. If now every character is put in correspondence with the vertex of the graph of the Mie automaton, and if there is a path from GA to that on the graph of the automaton, the vertex is connected by an arc with a vertex directed from M. At the beginning of the arc, the conjunction X () formed for this path is written; At the end of the arc, a subset of the operations Y () is formed from the operator vertex through which the path / 8 / passes.
The general algorithm for constructing monitors for the A system is graphically shown in Fig. 2. The description of the process in the form of OS or GAW leads often to a significant duplication of the same operations when they are written. In this regard, the synthesis of the automaton for the monitor displays in a compact form the OS or GAW in the system of Boolean functions. Consequently, the system of Boolean functions is a control table for the implementation of monitors of A-systems in the form of automata with store memory.
The algorithmic model of solving the problems of designing and controlling the CC allows us to carry out the design of the control process of the SS and control of the software equipment. Such a scheme allows you to flexibly and without additional costs to develop new software tools to manage the object taking into account the impact of external factors on the production system, in particular on the production process. Thus, a complex study of objects is necessary, starting with preliminary study, obtaining adequate models, algorithmizing processes and ending creation of effective management systems. Consequently, the algorithmization of management processes with the use of modern computer technology requires not only the improvement of management at all levels, but also the creation of new effective methods of rational and adequate description of research objects, optimization and construction of the control algorithm. Finally, consider the process of synthesizing automata for the implementation of algorithms for cryptography, methods and means of technical protection of information.
The algorithm is presented in the form of a graph-scheme of algorithms., Consisting of a set of operators-conditional and unconditional. We assume that the unconditional operators in the GSA correspond to the aggregates, and the conditional operators to the transitions between aggregates in the aggregate system, i.e. GAW is considered as an A-system
Thus, the main tasks are:
- Implementation of algorithms for cryptography, methods and means of technical protection of information based on programmable microcontrollers.
- Construction of control monitors based on finite state machines.
- Algorithmization of the design of the built-in systems of logical control of technological modules on the basis of the synthesis of control automata.
- Development of its PTC-programmer on the basis of well-known high-performance analogs and CAD-projecting system of programmable logic controllers.

III. EXPERIMENTAL RESULTS

In this paper, we propose the development of an algorithmic model of the transition from GAW to the table of Boolean functions. The transition from GAW algorithm AES to the table of Boolean functions based on the programming language JAVA, C ++, C #, C or PASCAL. The program is loaded into the BOOLEAN system using the OPEN button. The result is the table 1 implicants of systems of Boolean functions corresponding to the GAA of the AES encryption algorithm with the conditional operators x1, x2, ..., x6 and unconditional operators y1, y2, ..., y20.



X1	X2	X3	X4	X5	X6	X7	Y1	Y2	Y3	Y4	Y5	Y6	Y7	Y8	Y9	Y10	Y11	Y12	Y13	Y14	Y15	Y16	Y17	Y18	Y19	Y20
0	0	0	0	0	0	0	1	1	1	1	0	1	1	0	1	1	1	1	1	1	0	0	0	0	0	1
0	0	0	0	0	0	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	0	0	0	1	0	1
0	0	0	0	0	1	0	1	1	1	1	0	1	1	0	1	1	1	1	1	1	0	0	1	0	0	1
0	0	0	0	0	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	0	0	1	1	0	1
0	0	0	0	1	0	0	1	1	1	1	0	1	1	0	1	1	1	1	1	1	0	1	0	0	0	1
0	0	0	0	1	0	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	0	1	0	1	0	1
0	0	0	0	1	1	0	1	1	1	1	0	1	1	0	1	1	1	1	1	1	0	1	1	0	0	1
0	0	0	0	1	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	0	1	1	1	0	1
0	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	0	0	0	0	1
0	0	0	1	0	0	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	0	0	1	0	1
0	0	0	1	0	1	0	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	0	1	0	0	1
0	0	0	1	0	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	0	1	1	0	1
0	0	0	1	1	0	0	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	0	0	0	1
0	0	0	1	1	0	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	0	1	0	1
0	0	0	1	1	1	0	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	1	0	0	1
0	0	0	1	1	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1
0	0	1	0	0	0	0	1	1	1	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	1	1
0	0	1	0	0	0	1	1	1	1	1	0	1	1	0	1	0	0	0	0	0	0	0	0	1	1	1
0	0	1	0	0	1	0	1	1	1	1	0	1	1	0	1	0	0	0	0	0	0	0	1	0	1	1
0	0	1	0	0	1	1	1	1	1	1	0	1	1	0	1	0	0	0	0	0	0	0	1	1	1	1
0	0	1	0	1	0	0	1	1	1	1	0	1	1	0	1	0	0	0	0	0	0	1	0	0	1	1
1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1
1	1	1	0	1	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	1	0	0	1	1
1	1	1	0	1	0	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	1	0	1	1	1
1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	1	1	0	1	1
1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1
1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	1	1
1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	0	0	1	1	1
1	1	1	1	0	1	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	0	1	0	1	1
1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	0	1	1	1	1
1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1	0	0	1	1
1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1	0	1	1	1
1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	0	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1

Thus, in this paper, we propose the development of an algorithmic model of the transition from GAW to the table of Boolean functions, where the main tasks are consisting of

- Implementation of algorithms for cryptography, methods and means of technical protection of information based on programmable microcontrollers.
- Construction of control monitors based on finite state machines.
- Algorithmization of the design of the built-in systems of logical control of technological modules on the basis of the synthesis of control automata.
- Development of its PTC-programmer on the basis of well-known high-performance analogy and CAD-projecting system of programmable logic controllers.

IV.CONCLUSION

Thus, the article proposes an algorithmic method for designing embedded systems of logical control and information security by microprogram automata on matrix LSIs. On the basis of the graph-scheme of the AES cryptography algorithm, a table of implicants of systems of Boolean functions was constructed.

REFERENCES

[1] Buslenko N.P. “Modeling of complex systems.” - M .: Nauka, 1978, p. 390.

[2] Buslenko V.N., Kaganovich V.L., Dashkova V.G. “Questions of development of technology of aggregative modeling.” - Programming, 1988, №1, p. 66-76.

[3] Kabulov V.K. “Issues of formalization in the study of systems.” - Questions of cybernetics, issue 126, Tashkent: NPO Cybernetics, Academy of Sciences of the Uzbek SSR, 1984, pp.3-15.

[4] Kabulov V.K. “Questions of the standard description of systems and aggregative systems of NP Buslenko”. - Questions of cybernetics, issue 130, Tashkent: NPO "Cybernetics" of the Academy of Sciences of the Uzbek SSR, 1985, p.3-20.

[5] Mayorov S.A. and others. “Flexible automated production.”- M .: Machine Language, 1985, p.454

[6] Sklyarov V.A. “Synthesis of automata on matrix LSIs.” - M .: Science and technology, 1984, p.285.

[7] Baranov SM., Sklyarov V.A. “Digital devices on programmable LSI with a matrix structure.” - M .: Radio and communication 1986, p. 269.

[8] Baranov S.I. “Synthesis of firmware automata.” -L .: Energy, 1979, p. 231.

AUTHOR’S BIOGRAPHY

PhD Researcher, Dept. of Information Security, Faculty of Mathematics, National University of Uzbekistan named after Mirzo Ulugbek & City Tashkent, Uzbekistan