Measurements infrastructure Vol. 5 (2023) MI_024_260722

https://doi.org/10.33955/v5(2023)-024

Systems engineering of cyber-secured digital and information measuring systems based on the signature Boolean-polynomial algebra synthesis apparatus

Tupkalo Vitalii [1], Cherepkov Serhii [2]

[1] Kyiv University of Intellectual Property and Law of National University Odesa Law Academy, Ukraine
[2] SE «Ukrmetrteststandart», Ukraine

E-mail: tvn.prof@gmail.com

Abstract

Development of DIMSCC models with cyber-controllability of their apparatus and software for computing function (operations) in real time becomes the primary task since the problem relevance of the cyber security of digital information and measuring systems of control complexes (DIMSCC) for critical infrastructure objects is increasing. Based on an analysis of known digital systems functional control methods new term «functional cyber-controllability of the digital informational and measuring system» was defined in the article. New approach to operational functional control of hardware redundancy is proposed. This is the synthesis of DIMSCC computing operations. Hardware redundancy is a synthesized control node chosen for functional control of various DIMSCC basic arithmetic and logical functions (operations) which should be reduced to simple procedure of corresponding switching functionally complete combinational structures from a finite set (standard set). Concerning this, the synthesis task is as follows. Only inputs and outputs of specified object are available for functional control of arithmetic and logical operations on binary operands under external hacker influence. Combination type functional control node structure (operational compositional adaptation) should be developed depending on the type of controlled computing operation being performed. The result of the synthesis task solving is a system of formulae determination (signature control equations) of the signature functional control of all DIMSCC basic arithmetic and logical functions (operations) on a single basis of a single equivalent representation of their known formulaic expression by corresponding (adequate) descriptions in infix notation (infix models). Apparatus of Boolean-polynomial algebra is used aiming to realize infix notation. The practical advantage of the proposed approach to the synthesis of hardware redundancy of operational functional signature control of computing operations is the transition possibility from signature control equations formulae to their realization implementation in the form of a signature control node directly without additional interpreting and minimizing procedures use by simple logical composition (switching) functionally complete combinational structures from a finite set (standard set).

Published
05.05.23

Keywords: informational security, cyber security of information and measuring systems, functional cyber-controllability, computing functions operational control.

1. Introduction

Problem statement. Development of the cyber security of digital information and measuring systems of control complexes (DIMSCC) for critical infrastructure objects needs a new approach to functional control (FC) task solving. Simultaneously, ensuring high efficiency and reliability in detecting hacker incidents in real-time becomes a priority. So, DIMSCC synthesis models should allow ensuring their functional cyber-controllability.

One of the FC methods development constraining factors in circumstances of continuous complication and integration level of DIMSCC digital elements base increase is an attempt to use known mathematical apparatus based on the automated model of functional control objects (FCO).

Input conditions for the proposed approach are DIMSCC functional control objects (FCO) access possibility with its external connections only. Thus, synthesis of (control node CN) structural (hardware) redundancy for FCO various controlled functions should be reduced to a simple procedure of corresponding switching of functionally complete combinational structures from a finite set (standard set).

2. Main body

Latest sources and publications research. The particular scope of works is known [1-9] in mentioned cyber-controllability problem context of various function digital systems in real-time (operational FC), which considers the choice of mathematical substantiation for hardware control by using hardware and informational (code) redundancy related to various typical computing devices and digital control automatic devices of a general type. Though, the general theory of informational systems operational FC ability to detect a targeted violation of their proper functioning due to telecommunications influence (cyber attacks) is absent in these works.

Several ways to solve the complex DIMSMC secure functioning problem exist, for example, using multiple backups of databases method, code, and numerical control in the module of digital data transmission, hashing, etc. [10]. Particular problems should be mentioned in the development process of the complicated systems mathematical models, including DIMSCC [11]. In particular, these models are connected with the asynchronous parallel processes, numerous internal connections between system elements, plenty of its parameters, and various non-linear restrictions. Mentioned methods used to analyze such systems control characteristics result in real processes substantially causing simplification and consequently discredit the developed model conformity.

Unsolved part of the general problem. The unified methodological (system engineering) base for all arithmetic operations in digital systems is primary addition operations and register shift [12]. Though, it should be noted that the register shift operation reduces the speed of arithmetic operations. So, in mentioned general problem context, authors propose apparatus redundancy synthesis abstraction models for functional control of selected DIMSCC operations (both arithmetic and Boolean logic) represented by corresponding (adequate) descriptions in infix notation (infix models) as determined control arithmetic functions. Such a proposal comes from the development trend of modern DIMSCC based on complete unification and standardization of signal structures and interfaces principles [13].

The research goal is grounding and forming a proposition for the further development direction of DIMSCC cyber secured system engineering by unified structural FC redundancy based on author's «signature Boolean polynomic algebra» synthesis apparatus.

Task statement. The following definition is proposed according to the goal.

Definition 1. Functional cyber-controllability of the digital informational measuring system of the critical infrastructure object control complex is system characteristics that describes the suitability of part or all of the target computing functions $f_i \in F(X_{[n]})$ inherent in it over n-bit operands $X_{[n]}$ before detecting hacker intervention (incidents) in the process of performing f_i functions by functional control means in real-time.

In Definition 1 context DIMSCC functional control model is presented in Fig. 1.

This model includes: the functional control object (FCO), that is, the automatic digital device (DIMSCC arithmetic logic module) with ψ a transmitting function; the control node (CN) consists of three combinational schemes (hardware redundancy),

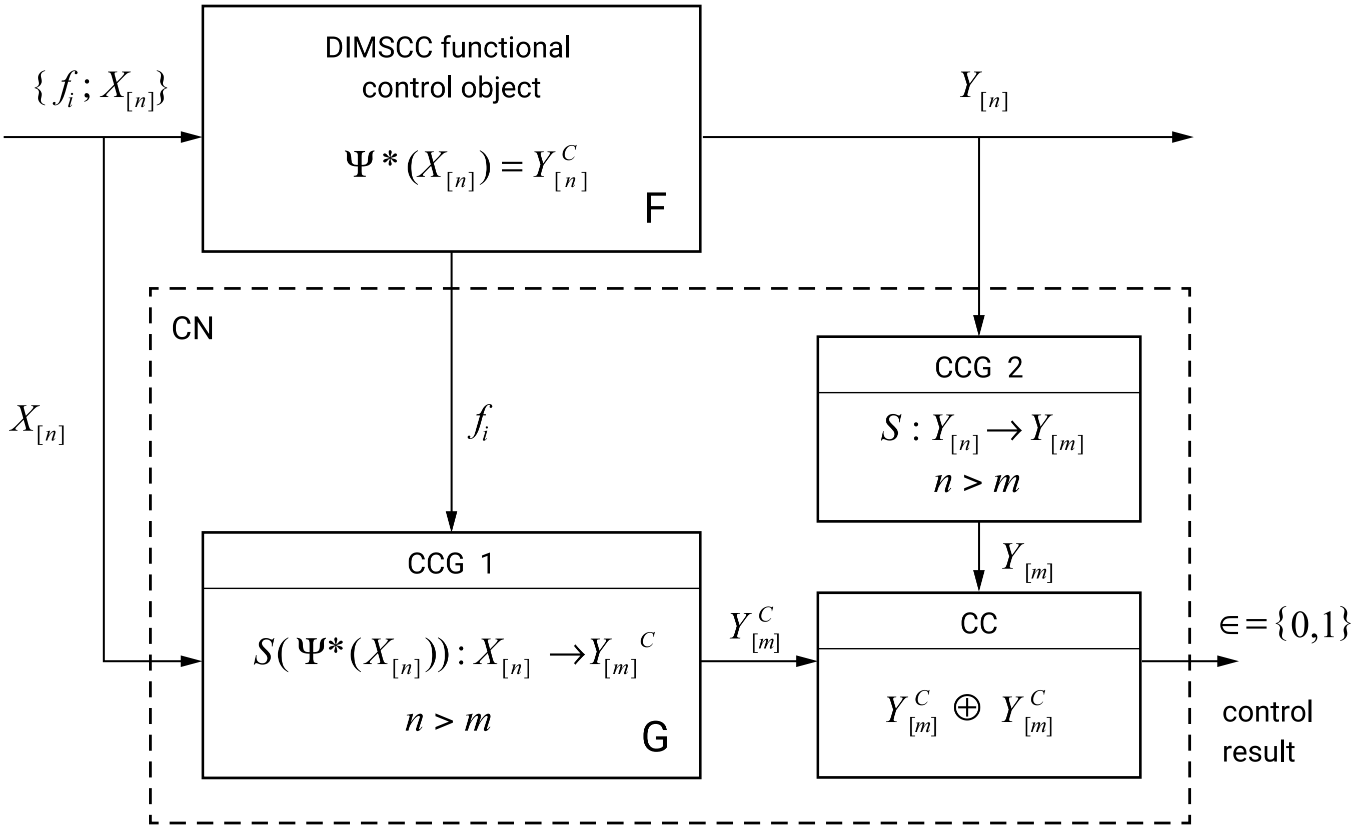


Fig. 1. *Functional control model (authors model)*

which depending on f_i the control function type performs a surjective reflection with the control characteristics generator CCG 1:

$$S(\Psi*(X_{[n]})): X_{[n]} \to Y_{[m]}{}^C \tag{1}$$

of n length input binary vectors $X_{[n]}$ into $m(n > m)$ length output binary vectors $Y_{[m]}{}^C$ according to f_i names (codes) from FCO F set of controlled operations performs a surjective reflection with the control characteristics generator CCG 2:

$$S: Y_{[n]} \to Y_{[m]} \tag{2}$$

of n length input binary vectors $Y_{[n]}$ into m length output binary vectors $Y_{[m]}$; the operator S is necessary for n length vectors encoding into corresponding m length vectors to ensure specified functional control probability; m-bit codes comparator (CC) performs reflection:

$$\delta_{CC}: (Y_{[m]}{}^C \oplus Y_{[m]}) \to \in \{0,1\} \tag{3}$$

by identifying the correspondence of each FCO output vector $y_i \in Y_{[m]}$ with the corresponding vectors $y_{ci} \in Y_{[m]}{}^C$.

According to the specification requirements for the standard set of combinational elements for CN synthesis, we define the dependence of functions $\Psi(X_{[n]})$ and $\Psi*(X_{[n]})$ as infix notation:

$$\Psi(X_{[n]}) = \Psi*(X_{[n]}) = (\psi_1 * \psi_2 * ... * \psi_q), \tag{4}$$

where

$*$ and ψ_j are Boolean superposition (commutation) operation and the jth elementary Boolean component of the universal representation by the Boolean equivalent of the F set of DIMSCC target controlled arithmetic and logical operations correspondingly.

So, the aim of DIMSCC cyber-controllability ensuring is as follows: let inputs and outputs of a given FCO be controllable. It is necessary to specify the set of G control characteristics for all possible F set operations executed by this FCO for CCG1 synthesis with characteristics of controlled functions $\Psi(X_{[n]})$ from F the set that could be presented by corresponding equivalent Boolean function (4) and operator S allowing surjective reflection according to the superposition principle:

$$S(\Psi(X_{[n]}))=S(\Psi*(X_{[n]}))=S\psi_1*S\psi_2*\ldots*S\psi_q. \tag{5}$$

Fundamental result. Synthesis problem solution (5) is based on the mathematical apparatus of the author's signature Boolean-polynomial algebra (signature algebra by V. Tupkalo). The definition is the following [14].

Definition 2. Signature Boolean-polynomial algebra is surjective reflection algebra over the GSF (Galois Signature Field) $(n\,,\ m)$ finite set of binary numbers of n length from signature (sig) of $m\left(n>m\right)$ length, the basic set of algebra is the system set:

$$W=(R;\oplus,H,H^1,sig,\alpha,\beta,\varphi) \tag{6}$$

where:

- R – set of DIMS arithmetical and logical functions, which are selected functional control objects (operational in time);
- two binary logical operations are addition by modulus two and the logical operation of forming the mutual polynomial characteristic (H) of two numbers involved in arithmetic addition operation;
- two unary operations: one-bit truncation operation of the left most significant digit of the mutual polynomial characteristic (H^1) number if the condition requires performing a particular controlled arithmetic operation on a pair of binary numbers in the model (7) context; combinational type operation of a binary number signature (sig) forming;
- φ three n-bit constants: φ-binary number with a unit only in the least significant digit, α – binary number with units in all digits (inverting constant), β – binary number with a unit only in the most significant digit.

Statement 1. Determine arithmetic function $\Psi(X)$ may correspond to the S-transform of its Boolean equivalent in infix form (5) if every function ψ_j is unary or binary, the operator S is linear, and the $*$ operation is addition by modulus two.

Statement 1 proof is in the Appendix.

According to Statement 1 Boolean equivalent of the arithmetic addition function $F^{(+)}$ is as follows:

$$A+B=(A\oplus B)\oplus H(A+B)=A\oplus B\oplus H(A+B) \tag{7}$$

where:

$H(A+B)$ – number, which code characterizes shift units transition during the A and B numbers adding operation.

Since $H(A+B)$ establishes a mutual polynomial connection between the A and B numbers and signature algebra defines $H(A+B)$ as mutual polynomial characteristic of two numbers involved in the arithmetic addition operation.

Example:

$A_{[7]}=1010111$ or $A\left(x\right)=x^7+x^5+x^3+x^2+1$;
$B_{[7]}=0110001$ or $B\left(x\right)=x^6+x^5+1$.

Addition and calculation of two numbers mutual polynomial characteristic result is:

$$A+B=\left(\begin{array}{l}\leftarrow\leftarrow\leftarrow\;\;\leftarrow\leftarrow\leftarrow\\ \vdots\,1\,0\,1\,0\,1\,1\,1\\ \vdots+\\ \vdots\,0\,1\,1\,0\,0\,0\,1\end{array}\right)=\mathbf{1}\,0\,0\,0\,1\,0\,0\,0$$

$$H_{[8]}=\mathbf{1}\vdots\,1\,1\,0\,1\,1\,1\,0$$

Then the arithmetic sum of the A and B numbers according to (7) through Boolean operation «modulus two sum» is as follows:

$$A_{[8]}+B_{[8]}=\mathbf{0}1010111\oplus\mathbf{0}0110001\oplus$$
$$\oplus\,\mathbf{1}1101110=\mathbf{1}0001000.$$

It should be noted that if operands A and B of the arithmetic addition operations are presented by nth degree polynomials, then their $H(A+B)$ characteristic may be presented by $(n+1)$ degree polynomial. Thus, the synthesis task of $H(A+B)$ the characteristic generator is the development of a combinational node realizing Boolean function system on its outputs:

$$\begin{cases} h_1 = 0; \\ h_2 = a_1 b_1; \\ h_{i>2} = h_{i-1}(a_{i-1} \vee b_{i-1}).\ i\ =\ 3,\ \ldots,\ n+1. \end{cases} \qquad (8)$$

According to (8) general scheme of $H(A+B)$ characteristic generator is presented in Boolean basis «OR-AND» in Fig. 2.

In the Statement 1 regarding the requirement for S operator linearity context, the following should be noted. In [15], this operator may be linear in the case of its vector interpretation (sig) as a unary convolution operation of the binary number A of n length into its control characteristic of m length by the modulus of an irreducible primitive m degree polynomial $P^m(x)$ based on a recurrent (sequential clock in time), for example, a register shift algorithm with feedback. Though, this algorithm does not allow to realize synthesis of the parallel signature generator of binary n-bit numbers $A(x)$, which is necessary for functional control of high efficiency and reliability of detection hacker incidents during DIMS operation in real-time.

Based on this note, synthesis method of the parallel signature generator based on signature generating a matrix of an irreducible primitive polynomial $P^m(x)$ is proposed.

Definition 3. Generating signature matrix $M(sigA_{[n]})$ of the polynomial $P^m(x)$ is $(m\times n)$ a size matrix n, resulting from row-by-row multiplication of the column vector matrix of n-bit number $A_{[n]}$ with n rows of matrix $M(sigA_{[n]})$ of recurrent generation n vector rows of m-bit signature $sig\beta_{[n]}$ of binary number $\beta_{[n]}$ with the unit in the most significant digit (signature algebra constant).

In the Definition 3 context, the general model of the proposed synthesis generator signature matrix method is presented by equality (9), which has the corresponding matrix representation (10):

$$sigA_{[n]} = a_n sig\beta_{[n]} \oplus a_{n-1} sig\beta_{[n-1]} \oplus \ldots \oplus a_1 sig\beta_{[1]}; \qquad (9)$$

$$\begin{bmatrix} M(sigA_{[n]}) \\ P^m(x) \end{bmatrix} = \begin{bmatrix} M(sig\beta_{[n]}) \\ P^m(x) \end{bmatrix} \times \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \qquad (10)$$

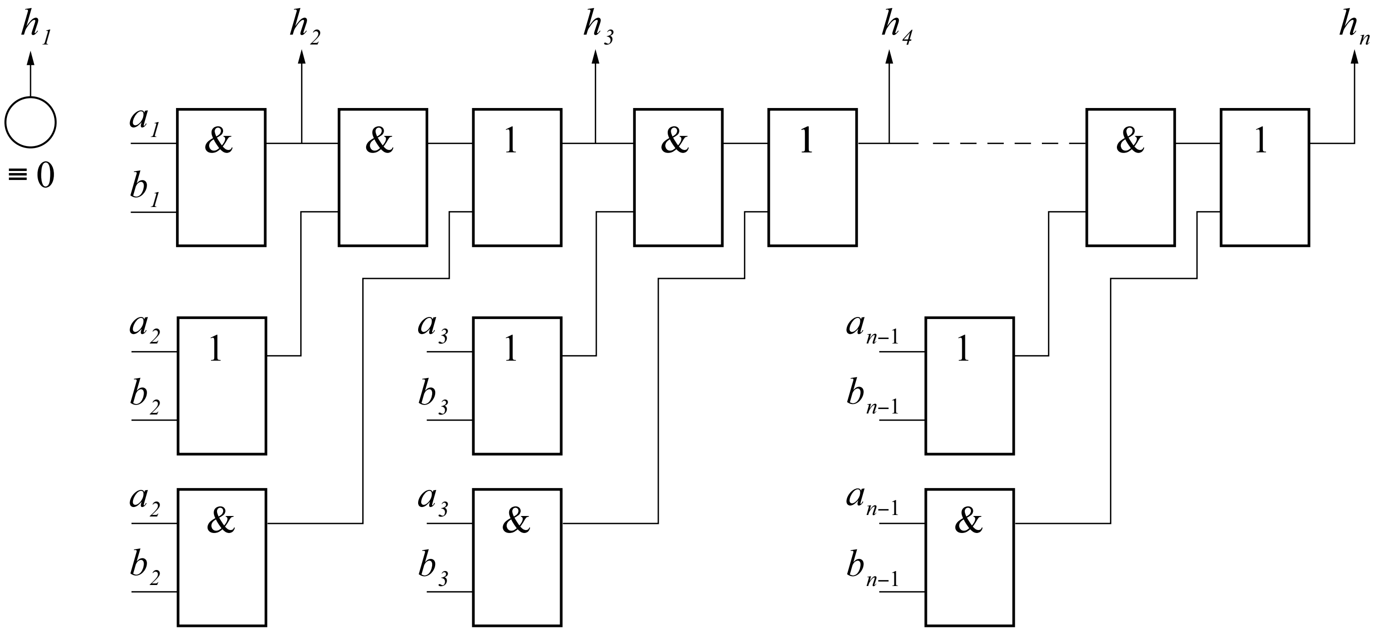


Fig. 2. *Scheme of $H(A+B)$ characteristic generator is presented in Boolean basis «OR-AND» (authors model)*

$$= \begin{bmatrix} sig\beta_{[1]} \\ sig\beta_{[2]} \\ \vdots \\ sig\beta_{[n]} \\ \mathbf{m} \end{bmatrix} \times \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 00\ldots0a_1 \\ 0a_2\ldots00 \\ \vdots \\ a_n0\ldots a_n0 \\ \mathbf{m} \end{bmatrix}\mathbf{n}.$$

Example: $A_{[6]} = 110110$.

Then we have:

$$a_6\beta_{[6]}\oplus a_5\beta_{[5]}\oplus a_4\beta_{[4]}\oplus a_3\beta_{[3]}\oplus a_2\beta_{[2]}\oplus a_1\beta_{[1]} =$$

$$= \left\{ \begin{array}{c:r} 1 & 100000 \\ 1 & 10000 \\ \cancel{0} & \cancel{1000\ \oplus} \\ 1 & 100 \\ 1 & 10 \\ \cancel{0} & \cancel{1} \end{array} \right\}$$

$$A = \;\; 110110$$

According to (10), the method of the synthesis generator parallel type-signature based on the signature generating matrix of an irreducible primitive polynomial is presented in Fig. 3, 4, 5 correspondingly.

Based on the models of signature creation in Fig. 3–5, the constant is $\beta_{[n]} \in W$.

Definition 4. The signature (sig) of the binary number $A(x)$ is its convolution (linear transformation $sigA(x)$) based on signature generating the matrix of an irreducible primitive polynomial.

Signature definition interpretation allows ensuring of the reliability control task is reduced to the known task of an irreducible primitive polynomial $P^m(x)$ type choice and parallel signature generator synthesis task to be reduced to the combinational logical convolution node of the pyramidal type construction. Herewith, node degree number and, thus, the signature generating operation time depends on the ratio of n digits of

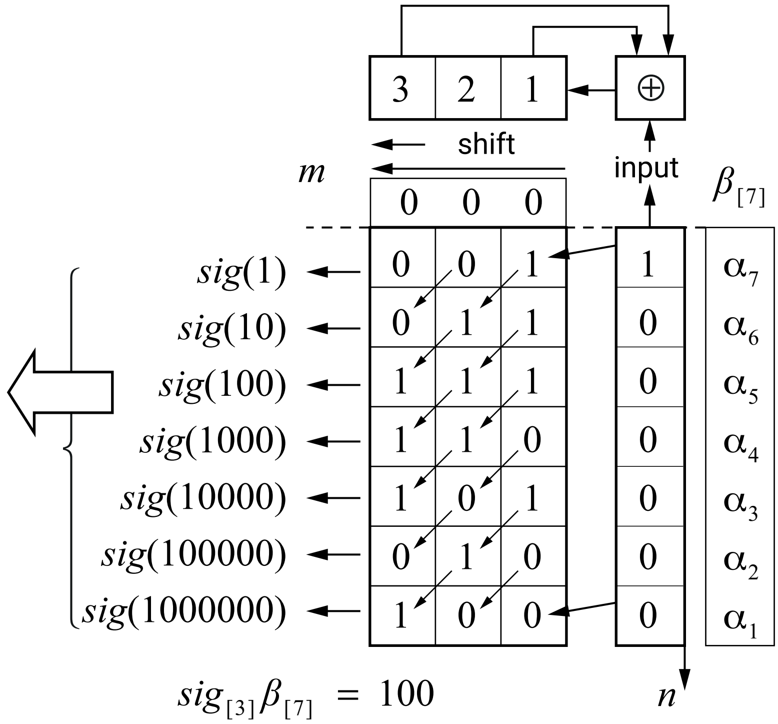
Methodology of creating a parallel-type signature generator

Step 1: selection of a sequential (recursive) generation model
n vector rows of m - bit signature

$$sigA_{[n]} = a_n sig\beta_{[n]} \oplus a_{n-1} sig\beta_{[n-1]} \oplus \ldots \oplus a_1 sig\beta_{[1]}$$

Example: $P(x) = x^3 + x + 1, \quad n = 7$

$$M(sig_{[3]}\beta_{[7]}) = \begin{bmatrix} sig\beta_{[1]} \\ sig\beta_{[2]} \\ sig\beta_{[3]} \\ sig\beta_{[4]} \\ sig\beta_{[5]} \\ sig\beta_{[6]} \\ sig\beta_{[7]} \end{bmatrix} = \begin{bmatrix} 001 \\ 011 \\ 111 \\ 110 \\ 101 \\ 010 \\ 100 \end{bmatrix}$$



$sig(1)$	0	0	1	1	α_7
$sig(10)$	0	1	1	0	α_6
$sig(100)$	1	1	1	0	α_5
$sig(1000)$	1	1	0	0	α_4
$sig(10000)$	1	0	1	0	α_3
$sig(100000)$	0	1	0	0	α_2
$sig(1000000)$	1	0	0	0	α_1

$$sig_{[3]}\beta_{[7]} = 100$$

Fig. 3. *Methodology for creating a parallel-type signature generator: Step 1 (authors model)*

the input number $A(x)$ and the bit rate m of the signature code (selected polynomial degree $P^m(x)$).

Then considering (7), for addition function $F^{(+)}$ signature control formula is in the form:

$$sig(A+B)=sig(A\oplus B)\oplus sigH(A+B)= \qquad (11)$$
$$=sigA\oplus sigB\oplus sigH(A+B)$$

and operators $\{\oplus, sig, H(...)\}\in W$.

Subtraction function $F^{(-)}=A-B=A+(-B)$. Let us use the known method of subtracting binary numbers using an additional subtractor [16] code in the synthesis process of arithmetic binary numbers subtraction operation control formula. In this case, signature algebra formula converting the direct n-bit code of the modulus of the subtractor $(-B)$ number into its additional code $(-B)_{ADD}$ modulus two sum:

$$(-B)_{ADD}=(B\oplus\alpha)\oplus\varphi\oplus H^{1}[(B\oplus\alpha)+\varphi],$$

where mutual truncated polynomial characteristic $H^1[...]$ use prevents obtaining false results from generating operation $(-B)_{ADD}$ due to the possible digit grid expansion of the result by one higher digit. The following example demonstrates it:

$A_{[5]}-B_{[5]}=11011-01101=\mathbf{01110}=C_{[5]}$ – true result.

In the case of using the signature algebra apparatus, we have:

$$A-B=A+(-B)=A+(-B)_{ADD}=$$
$$=A+(B\oplus\alpha)\oplus\varphi\oplus H^{1}[(B\oplus\alpha)+\varphi]\ =$$

Methodology of creating a parallel-type signature generator

Step 2: Formation of the Generator Matrix of Signatures $M(sig_{[m]}A(x)_{[n]})$

Example: $P(x)=x^3+x+1, \quad n=7$

$$\begin{array}{ccccccccc} & & & & M(sig_{[3]}\beta_{[7]}) & & A(x)_{[7]} & & M(sig_{[3]}A(x)_{[7]}) \\ \Big[\ S(7,3)\ \Big] & = & \Big[\ M(sig_{[3]}A(x)_{[7]})\ \Big] & = & \begin{bmatrix}0\,0\,1\\0\,1\,1\\1\,1\,1\\1\,1\,0\\1\,0\,1\\0\,1\,0\\1\,0\,0\end{bmatrix} & \times & \begin{bmatrix}\alpha_1\\\alpha_2\\\alpha_3\\\alpha_4\\\alpha_5\\\alpha_6\\\alpha_7\end{bmatrix} & = & \begin{bmatrix}0&0&\alpha_1\\0&\alpha_2&\alpha_2\\\alpha_3&\alpha_3&\alpha_3\\\alpha_4&\alpha_4&0\\\alpha_5&0&\alpha_5\\0&\alpha_6&0\\\alpha_7&0&0\end{bmatrix} \\ & & & & & & & & \overline{\ S_3\quad S_2\quad S_1\ } \end{array}$$

System of logical equations construction of parallel-type signature generator

$sig_{[3]}A(x)_{[7]}$

$$\begin{cases} S_3 = \alpha_7\oplus\alpha_5\oplus\alpha_4\oplus\alpha_3 \\ S_2 = \alpha_6\oplus\alpha_4\oplus\alpha_3\oplus\alpha_2 \\ S_1 = \alpha_5\oplus\alpha_3\oplus\alpha_2\oplus\alpha_1 \end{cases}$$

Fig. 4. *Methodology for creating a parallel-type signature generator: Step 2 (authors model)*

Combinatorial parallel generator of field signatures GSF *(7, P³(x))*

$$sig_{[3]}A(x)_{[7]} = \begin{cases} S_3 = \alpha_7 \oplus \alpha_5 \oplus \alpha_4 \oplus \alpha_3 \\ S_2 = \alpha_6 \oplus \alpha_4 \oplus \alpha_3 \oplus \alpha_2 \\ S_1 = \alpha_5 \oplus \alpha_3 \oplus \alpha_2 \oplus \alpha_1 \end{cases}$$

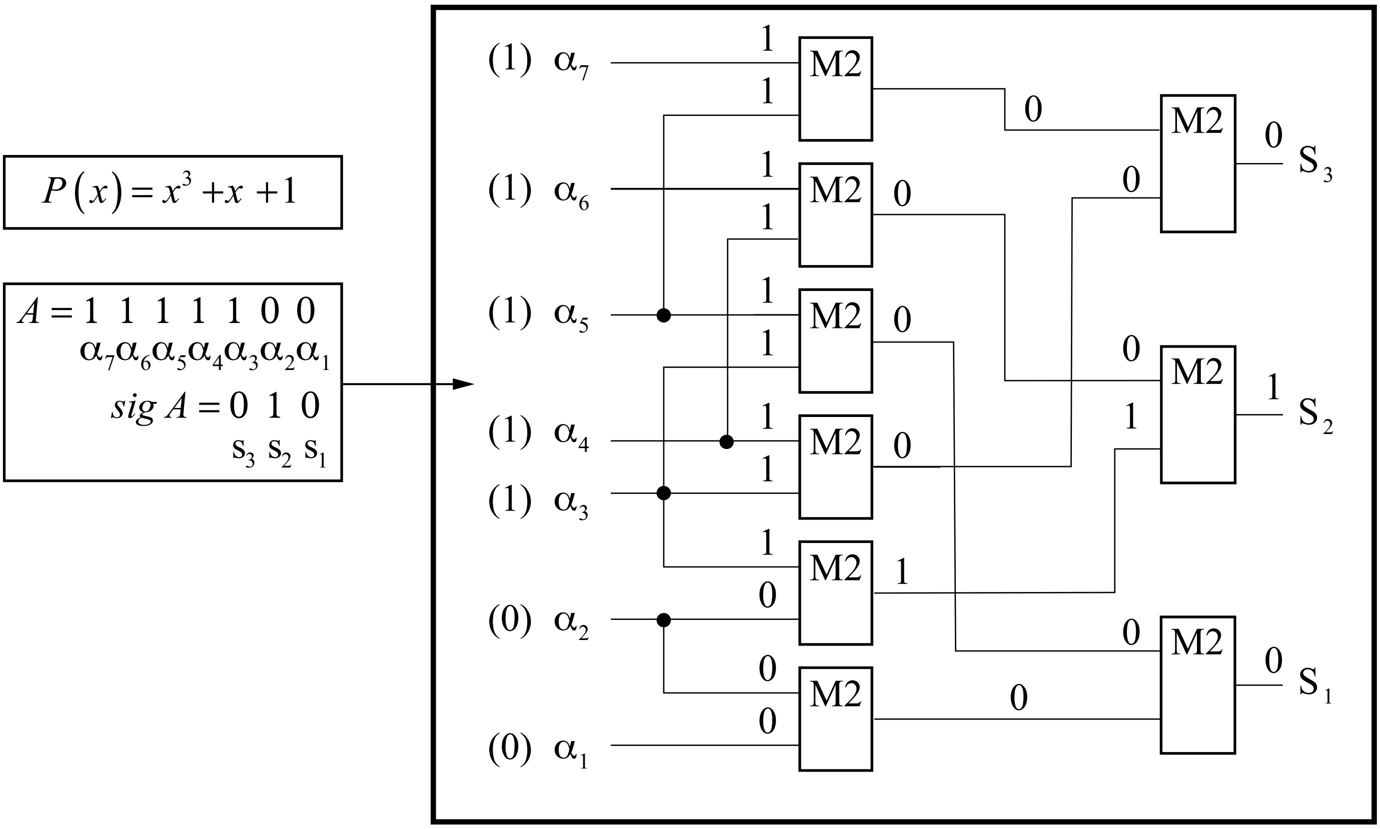


Fig. 5. *Combinatorial parallel generator of field signatures GSF (7, P³(x)) (authors model)*

$$= 11011 + \{(01101 \oplus 11111) \oplus 00001 \oplus$$

$$\oplus H^1\left[(10010) + 00001\right]\} = 11011 + 10011 =$$

$$= 11011 \oplus 10011 \oplus H^1[11011 + 10011] =$$

$$= 01000 \oplus \left[\begin{array}{r} \overset{\leftarrow}{1}\,1\,0\,\overset{\leftarrow}{1}\,\overset{\leftarrow}{1} \\ 1\,0\,0\,1\,1 \\ \hline \mathbf{1}\underbrace{0\,0\,1\,1\,0}_{} \end{array}\right] = 01000 \oplus \mathbf{00110} = \mathbf{01110},$$

$$H^1[\ldots]$$

so subtraction operation of binary numbers by algorithm according to used signature algebra formula is correct.

This example follows that this is the one-bit truncation operation of the left most significant digit of a number of the mutual polynomial characteristic.

Based on the above signature control formula of the binary numbers subtraction operation is as follows:

$$sig(A - B) = sigA \oplus sigB \oplus sig(\alpha \oplus \varphi) \oplus$$
$$\oplus\ sigH^1[(B \oplus \alpha) + \varphi] \oplus$$
$$\oplus sigH^1\{A + [B \oplus \alpha \oplus \varphi \oplus H^1[(B \oplus \alpha) + \varphi]]\}. \qquad (12)$$

The signature control formula (12) validity check example is in Appendix.

Multiplication function $F^{(X)} = (A \times B)$. Considering the ancient Egyptian method of multiplication [12] when establishing the weights of the digits of the multiplier:

$$B(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_2 x^2 + b_1 x;$$

$$A \times B = A \sum_{i=1}^{n} b_i 2^{i-1}.$$

Then based on (11) for positive cofactors, we have the control equation (signature control formula):

$$sig(A\times B)= \tag{13}$$
$$=\Big[\Big\{sigAb_1 2^0\oplus sigAb_2 2^1\oplus sigH[Ab_1 2^0+Ab_2 2^1]\Big\}_{\mathrm{sig}\Sigma_1}\oplus$$
$$\oplus\ sigAb_3\, 2^2\oplus sigH[\Sigma_1+Ab_3 2^2]\Big]_{\mathrm{sig}\Sigma_2}\oplus$$
$$\oplus\Big[\Big\{sig\Sigma_2\oplus sigAb_4 2^3\oplus sigH[\Sigma_2+Ab_4 2^3]\Big\}_{\mathrm{sig}\Sigma_3}\oplus$$
$$\oplus sigAb_5 2^4\oplus sigH[\Sigma_3+Ab_5 2^4]\Big]_{\mathrm{sig}\Sigma_4}\oplus\ldots\oplus$$
$$\oplus\Big[\Big\{sig\Sigma_{n-3}\oplus sigAb_{n-1}2^{n-2}\oplus sigH[\Sigma_{n-3}+Ab_{n-1}2^{n-2}]\Big\}_{\mathrm{sig}\Sigma_{-2}}\oplus$$
$$\oplus\ sigAb_n 2^{n-1}\oplus sigH[\Sigma_{n-2}+Ab_n 2^{n-1}]\Big]_{\mathrm{sig}\Sigma_{\mathrm{n-1}}}$$

In the case of different cofactor sign digits, the general representation of the multiplication results as modulus two superposition is the following:

$$F^{(x)}=(|A|\times|B|)+\beta_{[2n+1]}= \tag{14}$$
$$=(|A|\times|B|)\oplus\beta_{[2n+1]}\oplus H[(|A|\times|B|)+\beta_{[2n+1]},$$

where:

$\beta_{[2n+1]}-(2n+1)$ – digit number representing the sign digit, provided that it is located to the left of the mantissa most significant digit

The signature control formula (13) validity check example is in Appendix.

Division function $F^{(:)}=(A/B)$. Certainly, any binary dividend A can be uniquely represented in the form: dividend $A=BC+Z$, where B is divisor; C is quotient; Z is the rest. So, the division result regarding the rest is reduced to difference: $-Z=BC-A$. Then considering (12), we have the following equation system:

$$\begin{cases} sig(-Z)=sig(Z\oplus\alpha)\oplus sig\varphi\oplus sigH^{\mathbf{1}}[(Z\oplus\alpha)+\varphi];\\ sig(-A)=sig(A\oplus\alpha)sig\varphi\oplus sigH^{\mathbf{1}}[(A\oplus\alpha)+\varphi];\\ sig(BC-A)=sigBC\oplus sigA\oplus sig\alpha\oplus sig\varphi\oplus\\ \oplus sig\ H^{\mathbf{1}}[(A\oplus\alpha)+\varphi]sigH^{\mathbf{1}}\{BC+[A\oplus\alpha\oplus\varphi\oplus\\ \oplus H^{\mathbf{1}}[(A\oplus\alpha)+\varphi]]\}. \end{cases} \tag{15}$$

Then signature control division formula $F^{(:)}$ can be reduced to the signature equality control:

$$sig(-Z)=sig(BC-A)=sig\{BC\oplus A(\alpha\oplus\varphi)\oplus \tag{16}$$
$$\oplus H^{\mathbf{1}}[(A\oplus\alpha)+\varphi]\oplus H^{\mathbf{1}}\{BC+[A\oplus\alpha\oplus\varphi\oplus$$
$$\oplus H^{\mathbf{1}}[(A\oplus\alpha)+\varphi]]\}\}.$$

The signature control formula (16) validity check example is in Appendix.

Logical functions signature control. Comparing Boolean and Zhehalkin algebras follows [17], that basic set of two-digit logical functions (operations) of digital automatic devices of various purposes is a conjunction ($\wedge$), a disjunction ($\vee$) and modulus two sum ($\oplus$).

Function $F^{(\oplus)}=(A\oplus B)$. This function has an equivalent expression in signature algebra:

$$(A\oplus B)=(A+B)-2(A\wedge B)=(A+B)+(D)_{\mathrm{ADD}} \tag{17}$$

where analogical to (12):

$$(D)_{\mathrm{ADD}}=(D\oplus\alpha)\oplus\varphi\oplus H^{\mathbf{1}}[(D\oplus\alpha)+\varphi]; \tag{17.1}$$
$$D=(A\wedge B)\oplus(A\wedge B)H^{\mathbf{1}}[(A\wedge B)+(A\wedge B)].$$

As a result of expanding expression (17) by embedding, we obtain the following signature control formula of the function $F^{(\oplus)}$ execution:

$$sig(A\oplus B)=sigA\oplus sigB\oplus sigH^1\big[A+B\big]\oplus \tag{18}$$
$$\oplus\ sig\,H^1\big[(A\wedge B)+(A\wedge B)\big]\oplus sig(\alpha\oplus\varphi)\oplus$$
$$\oplus\ sig\,H^1\Big[H^1\big[(A\wedge B)+(A\wedge B)\big]\oplus\alpha\big)+\varphi\Big]\oplus$$
$$\oplus\ sig\,H^1\{(A\oplus B\oplus H^1\big[A+B\big])+$$
$$+(H^1\big[(A\wedge B)+(A\wedge B)\big]\oplus\alpha\oplus\varphi\oplus$$
$$\oplus H^1[(H^1[(A\wedge B)+(A\wedge B)]\oplus\alpha)+\varphi])\}.$$

Let us check the control formula (16) validity on the example of the input data:

$$A=1011110,\ B=0111111,\ (A\oplus B)=1100001,$$
$$P(x)=x^3+x+1.$$

The control operation result is the following:

(18.1)

$$\mathrm{sig}(1011110 \oplus 0111111) =$$

$$= sig\left(1011110\right) \oplus sig\left(0111111\right) \oplus sig\left(1111100\right) \oplus$$

$$\oplus sig\left(0111100\right) \oplus sig\left(1111110\right) \oplus sig\left(0000110\right) \oplus$$

$$sig\left(0111000\right);$$

$$\mathbf{111} = 011 \oplus 100 \oplus 010 \oplus 110 \oplus 001 \oplus 100 \oplus 001 = \mathbf{111}$$

Control formula (18) validity is verified.

It should be noted that the following equation could be chosen as the signature control formula of the function $F^{(\oplus)}$ execution:

$$sig(A \oplus B) = sigA \oplus sigB \ . \qquad (19)$$

Let us evaluate this possibility using the example of the previous data.

$$sig(1011110 \oplus 0111111) =$$

$$= sig\left(1011110\right) \oplus sig\left(0111111\right);$$

$$\mathbf{111} = 011 \oplus 100 = \mathbf{111}.$$

Let us consider the situation: operand A was distorted to $A_r = 0101100$ as a result of hacker intervention in operands A and B transferred directly to DIMSCC functional control object (Fig. 1) input. We have in this situation with signature functional control:

(19.1)

$$sig(0101100 \oplus 0111111) = sig\left(0010011\right) =$$

$$= sig\left(1011110\right) \oplus sig\left(0111111\right);$$

$$\mathbf{111} = 011 \oplus 100 = \mathbf{111}.$$

Thus, operation result error was not detected while control equation use (19). Moreover, code control by mod 2 would not work in this situation since the number of units in both codes of addition results by modulus two remained unchanged.

Known equation [18] could be used except (19):

$$(A \oplus B) \ = (A \wedge B) \oplus (A \vee B) \qquad (20)$$

and then the control equation is:

(21)

$$sig(A \oplus B) = sig(A \wedge B) \oplus sig(A \vee B).$$

Let us check the control formula (21) validity based on the previous data:

$$sig(1011110 \oplus 0111111) =$$

$$= sig(0011110) \oplus sig(1111111);$$

$$\mathbf{111} = 111 \oplus 000 = \mathbf{111}.$$

Let us check the control equation (21) controllability in such hacker intervention:

(21.1)

$$sig(0101100 \ \oplus \ 0111111) \ = sig\left(0010011\right) =$$

$$= sig\left(0101100\right) \oplus sig\left(0111111\right);$$

$$\mathbf{111} = 011 \oplus 100 \ \ = \mathbf{111}.$$

So, operation result error was not detected while the control equation (21) use.

Let us check the control equation (18) controllability in such hacker intervention that is as follows:

(22)

$$sig(A_r \oplus B) = sig \ A_r \oplus sigB \oplus sigH^1\left[A_r + B\right] \oplus$$

$$\oplus sigH^1\left[\left(A_r \wedge B\right) + \left(A_r \wedge B\right)\right] \oplus sig(\alpha \oplus \varphi) \oplus$$

$$\oplus sigH^1\left[(H^1[\left(A_r \wedge B\right) + \left(A_r \wedge B\right)] \oplus \alpha) + \varphi\right] \oplus$$

$$\oplus sigH^1\{(A_r \oplus B \oplus H^1[A_r + B\ ]) + (H^1[(A_r \wedge B) +$$

$$+ \ (A_r \wedge B)] \ \oplus \ \alpha \ \oplus \ \varphi \ \oplus \ H^1[(H^1[(A_r \wedge B) +$$

$$+ \ (A_r \wedge B)] \ \oplus \ \alpha) + \varphi])\}.$$

The control operation result is the following:

(22.1)

$$sig(0101100 \oplus 0111111) = sig\left(0101100\right) \oplus$$

$$\oplus sig\left(0111111\right) \oplus sig\left(1111000\right) \oplus$$

$$\oplus sig\left(1011000\right) \oplus sig\left(1111110\right) \oplus$$

$$\oplus sig\left(0001110\right) \oplus sig\left(1010000\right);$$

$$\mathbf{111} \neq 011 \oplus 100 \oplus 101 \oplus 111 \oplus 001 \oplus 010 \oplus 010 \ = \mathbf{100}.$$

Thereby, the signature control formula (18) use allowed detection of hacker intervention during logical operation $(A \oplus B)$ execution.

Signature control results (18.1), (19.1), (20.1) comparison proves that operation result error detection became possible due to signature control formula (19) and (18) insertion of «additional functional control filters» which are polynomial characteristics into formula (18). So, instead of Boolean linear polynomial signatures (19) and (20), the corresponding signature polynomial from signature algebra by V. Tupkalo set of the polynomials [14] was selected for functional control function $F^{(\oplus)}$ realization.

Definition 5. Signature formula as a modulus two sum of signatures is called a signature polynomial if at least one of the signatures is coupled with a mutual polynomial characteristic.

Definition 6. The signature polynomial is degenerate if it consists of only one or more units in signature (signatures) form mutual polynomial characteristic.

For example, the degenerated signature polynomial is:

$$sig\,(A+A) = sigH(A+A) = sig2A.$$

Function $F^{(\wedge)} = \left(A \wedge B\right)$. This signature algebra function is equivalent to:

$$\left(A \wedge B\right) = \left(A \vee B\right) - (A \oplus B) = \left(A \vee B\right) + (L)_{\text{ADD}}, \tag{23}$$

where:

$$(L)_{\text{ADD}} = (L \oplus \alpha) \oplus \varphi \oplus H^1[(L \oplus \alpha) + \varphi];$$
$$L = (A \oplus B).$$

As a result of expanding expression (23) by embedding, we obtain the following signature control formula of the function $F^{(\wedge)}$ execution:

$$\begin{gathered} sig\left(A \wedge B\right) = sig\left(A \vee B\right) \oplus sigA \oplus sigB \oplus \\ \oplus\, sig(\alpha \oplus \varphi) \oplus sigH^1\,[(A \oplus B \oplus \alpha) + \varphi] \oplus \\ \oplus\, sigH^1[(A \vee B) + (A \oplus B \oplus \alpha \oplus \varphi \oplus \\ \oplus\, H^1[(A \oplus B \oplus \alpha) + \varphi\,])] \end{gathered} \tag{24}$$

Let us check the control formula (24) validity on the example of the input data:

$$A = 1011110,\; B = 0111111,\; (A \wedge B) = 0011110,$$
$$P\left(x\right) = x^3 + x + 1.$$

The control operation result is the following:

$$\begin{gathered} sig(1011110 \wedge 0111111) = \\ = sig\,(1011110 \vee 0111111) \oplus sig\left(1011110\right) \oplus \\ \oplus\, sig\left(0111111\right) \oplus sig(1111110) \\ \oplus\, sig(000000) \oplus sig\left(0000000\right). \end{gathered}$$

$$\mathbf{111} = 000 \oplus 011 \oplus 100 \oplus 001 \oplus 000 \oplus 001 = \mathbf{111}.$$

Control formula (24) validity is verified.

Function $F^{(\vee)} = (A \vee B)$. According to (23) and definitions 5, 6 this signature algebra function is equivalent to:

$$\begin{gathered} (A \vee B) = (A \oplus B) + (A \wedge B) = \\ = (A \oplus B) - (A \wedge B) + 2(A \wedge B) = \\ = (A \oplus B) + (Q)_{\text{ADD}} + H^1[(A \wedge B) + (A \wedge B)], \end{gathered} \tag{25}$$

where by analogy with (23):

$$(Q)_{\text{ADD}} = (Q \oplus \alpha) \oplus \varphi \oplus H^1[\,(Q \oplus \alpha) + \varphi];$$
$$Q = (A \oplus B).$$

As a result of expanding expression (25) by embedding, we obtain the following signature control formula of the function $F^{(\vee)}$ execution:

$$\begin{gathered} sig\left(A \vee B\right) = sig(A \oplus B) \oplus sig(A \wedge B) \oplus \\ \oplus sig(\alpha \oplus \varphi) \oplus sigH^1[(A \wedge B) \oplus \alpha) + \varphi] \oplus \\ \oplus\, sigH^1\{(A \oplus B) + [(A \wedge B) \oplus \alpha \oplus \varphi \oplus \end{gathered} \tag{26}$$

$$\oplus H^1[(A \wedge B) \oplus \alpha) + \varphi]]\} \oplus$$

$$\oplus sigH^1[(A \wedge B) + (A \wedge B)] \oplus$$

$$\oplus sigH^1\{\{(A \oplus B) \oplus (A \wedge B) \oplus \alpha \oplus \varphi \oplus$$

$$\oplus H^1[((A \wedge B) \oplus \alpha) + \varphi]\} \oplus$$

$$\oplus H^1\{(A \oplus B) + [(A \wedge B) \oplus \alpha \oplus \varphi \oplus$$

$$\oplus H^1[((A \wedge B) \oplus \alpha) + \varphi]]\} +$$

$$+H^1[(A \wedge B) + (A \wedge B)]\}.$$

Let us check the control formula (26) validity on the example of the input data:

$$A = 1011110,\ B = 0111111,\ (A \wedge B) = 0011110,$$
$$P(x) = x^3 + x + 1.$$

The control operation result is the following:

$$sig(1111111) = sig(1100001) \oplus$$

$$\oplus sig(0011110) \oplus sig(1111110) \oplus$$

$$\oplus sig(0000010) \oplus sig(1000000) \oplus$$

$$\oplus sig(0111100) \oplus sig(0000000)$$

$$\mathbf{000} = 111 \oplus 111 \oplus 001 \oplus 011 \oplus 100 \oplus 110 \oplus 000 = \mathbf{000}.$$

Control formula (26) validity is verified.

3. Conclusions

The scientific novelty of the obtained theoretical results is the proposition of further development strategy for cyber-secured system engineering of digital information and measuring systems of control complexes (DIMSCC) for critical infrastructure objects by unified structural combinational type redundancy. So, the authors proposed to perform a structural redundancy synthesis problem solution by formulae system forming (signature control equations) of the signature functional control of all DIMSCC basic arithmetic and logical functions (operations) on a single basis of a single equivalent representation of their known formulaic expression by corresponding (adequate) descriptions in infix notation (infix models). The authors synthesis apparatus of «signature Boolean-polynomial algebra» is proved to be used aiming to realize infix notation. Practical advantage of the proposed approach to the synthesis of hardware redundancy of operational functional signature control of computing operations is the transition possibility from signature control equations formulae to their realization implementation in the form of a signature control node directly without additional interpreting and minimizing procedures use by simple logical composition (switching) functionally complete combinational structures from a finite set (standard set). Further development in this field includes DIMSCC hardware signature functional control method development to prevent hacker attacks.

4. Appendix

Statement 1 verification. Since the condition for equality (2) fulfillment is operator S from function $\Psi^*(X)$, independent selection, then Boolean equivalent existence of determined arithmetical function $\Psi(X)$ does not exclude its infix notation (1). In its turn, since continuous in time (continuous digital system timing) control is considered, then Hilbert's thirteenth problem solution means that any continuous function n-variables can be represented as the superposition of two variables continuous functions [15]. Then superposition (2) principle is realized if the linear S-transform of a linear Boolean function. Linearity of the Boolean equivalent (5) is possible in case all functions ψ_j are one and (or) two variables functions under conditions ψ_j and * sum by modulus two or equivalence[17].

Let us consider that S is not a surjective reflection. Then, at least one such vector $y_j{}^C \in Y_{[m]}{}^C$ should be on the comparator CC (Fig. 1) input and for all x_j on the CCG 1 input is $S(x_j) \neq y_j{}^C$. Though error-free CCG 1 transition into the operational state with such $y_j{}^C$ contradicts the functional (hardware) control organization essence:

$$S(\Psi^*(X_{[n]})) : X_{[n]} \to Y_{[m]}{}^C$$

that is surjective reflection, which was to be proved.

Example 1. Control formula (12) validity check.

Given:

$$A=110110,\quad B=011100,\quad (A-B)=011010,$$
$$\alpha=111111,\quad \varphi=000001,\quad P(x)=x^3+x+1,$$
$$sig(A-B)=000.$$

1. Found out $H^1[(B\oplus\alpha)+\varphi]$:

$$(B\oplus\alpha)=100011;$$

$$\left[\begin{array}{r} 1000\overset{\leftarrow}{1}\overset{\leftarrow}{1} \\ + \\ \underline{000001} \end{array}\right] H^1[\ \ldots]$$

$$H^1[(B\oplus\alpha)+\varphi]=000110$$

2. Found out $H^1\{A+[B\oplus\alpha\oplus\varphi\oplus H^1[(B\oplus\alpha)+\varphi]]\}$:

$$011100\oplus111111\oplus000001\oplus00110=100100;$$

$$\left[\begin{array}{r} \overset{\leftarrow}{1}0\overset{\leftarrow}{0}100 \\ + \\ \underline{110110} \end{array}\right] H^1\{\ldots\}$$

$$\mathbf{1}001000$$

$$H^1\{\ldots\}=001000$$

3. Let us find the difference $(A-B)^*$ by the Boolean equivalent formula:

$$(A-B)^*=A\oplus B\oplus\alpha\oplus\varphi\oplus H^1[\ldots]\oplus H^1\{\ldots\}=$$
$$=011010=(A-B).$$

4. Let us find the control characteristic of subtraction operation, formed by the control node CN (Fig. 1):

if $P(x)=x^3+x+1$ we obtain:

$$sig(A-B)^*=$$
$$=sigA\oplus sigB\oplus sig\alpha\oplus\varphi\oplus H^1[\ldots]\oplus H^1\{\ldots\}=$$
$$=011\oplus100\oplus100\oplus001\oplus100\oplus110=000=$$
$$=sig(A-B).$$

Equality (12) is verified.

Example 2. Signature control formula (13) validity check.

Given:

$$A=10111,\ B=11101,\ (A\times B)=1010011011,$$
$$P(x)=x^3+x+1,\ sig(A\times B)=111.$$

The multiplication result [12] when presenting the weights of the digits of the multiplier is the following:

$$\Sigma_1=Ab_1 2^0\oplus sigAb_2 2^1\oplus H\,[Ab_1 2^0+Ab_2 2^1]\ =$$
$$=0000010111$$

$$\Sigma_1=0000010111\oplus0000000000\oplus0000000000=$$
$$=0000010111$$

$$\Sigma_2=\Sigma_1\oplus Ab_3 2^2\oplus H[\Sigma_1+Ab_3 2^2]=0001110011$$

$$\Sigma_2=0000010111\oplus0001011100\oplus0000111000=$$
$$=0001110011$$

$$\Sigma_3=\Sigma_2\oplus Ab_4 2^3\oplus H\,[\Sigma_2+Ab_4 2^3\,]\ =\ 0111100000$$

$$\Sigma_3=0001110011\oplus0010111000\oplus0111100000=$$
$$=0100101011$$

$$\Sigma_4=(A\times B)^*=\Sigma_3\oplus Ab_5 2^4\oplus H[\Sigma_3+Ab_5 2^4]\ =$$
$$=0111100000$$

$$(A\times B)^*=\ 0100101011\ \oplus\ 0101110000\ \oplus$$
$$\oplus\ 1011000000\ =1010011011.$$

So,

$$(A\times B)^*=(A\times B),\ sig(A\times B)^*=sig(A\times B)=111.$$

Equality (13) is verified.

Example 3. Signature control formula (16) validity check.

Given:

$$A=BC+Z=1100011,\ B=0010010,$$
$$Z=0001001,\ C=0000101,\ BC=1011010,$$
$$\alpha=1111111,\ \varphi=0000001,\ P(x)=x^3+x+1.$$

Result:

1. Let us form the left side of the equation (16):

$$sig(-Z) = sig(Z \oplus \alpha) \oplus sig\varphi \oplus sigH^{1}[(Z \oplus \alpha)+\varphi] =$$

$$= 111 \oplus 001 \oplus 000 = \mathbf{110}.$$

2. Let us form the right side of the equation (16):

$$sig(BC - A) = sigB \oplus C\, sigA \oplus sig\alpha \oplus sig\varphi \oplus$$

$$\oplus sigH^{1}[(A \oplus \alpha)+\varphi] \oplus sigH^{1}\{BC + [A \oplus \alpha \oplus$$

$$\oplus\ \varphi \oplus H^{1}\,[(A \oplus \alpha) + \varphi]]\} =$$

$$= 100 \oplus 100 \oplus 000 \oplus 001 \oplus 111 \oplus 000 = \mathbf{110}.$$

Equality (16) is verified.

References

1. *Digital automatic device operation control. System codes* [Контроль работы цифрового автомата. Систематические коды]. (Accessed 20.06.2022). [In Russian] https://koralexand.ru/?page_id=129
2. *Control of information words use and their addresses by mod 3 in digital automation devices* [Применение контроля информационных слов и их адресов по mod 3 в цифровых устройствах автоматики]. (Accessed 20.06.2022). [In Russian] https://works.doklad.ru/view/MWsnskSFwF8/all.html
3. Bystrova I., Podkopayev B. 2020 *Errors localization in networks of digital devices* [Локализация ошибок в сетях из цифровых автоматов состояний]. Russian universities news. Radio electronics. **V. 23, № 1,** pp. 18-29. [In Russian]
4. Yakymets N., Kharchenko V. 2007 *Fault-tolerant digital control systems with programmable logic based on partially functional digital automation devices: models and implementation* [Отказоустойчивые цифровые системы управленияс программируемой логикой на основе частично работоспособных автоматов: модели и реализация]. National Aerospace University «Kharkiv Aviation Institute». Information processing systems. **Issue 4 (62),** pp. 134-138. [In Russian]
5. Fedikhin A., Cespedes Garsia P. 2018 *To the question of the fault-tolerant computers structure of stratus computer inc.* [К вопросу о структурах отказоустойчивых компьютеров фирмы stratus computer inc.]. Mathematical machines and systems. **№ 4,** pp. 87-100. [In Russian]
6. *Hardware control methods* [Методы аппаратурного контроля]. (Accessed 20.06.2022). [In Russian] https://studfile.net/preview/9099982/page:17/
7. *Program-logical control methods* [Программно-логические методы контроля]. (Accessed 20.06.2022). [In Russian] https://studfile.net/preview/9099982/page:18/
8. *Numerical and digital control* [Числовой и цифровой контроль]. (Accessed 20.06.2022). [In Russian] https://studfile.net/preview/4354159/page:15/
9. *Particular modulus control cases. Methods for constructing convolution schemes* [Частные случаи контроля по модулю. Способы построения схем сверток]. (Accessed 20.06.2022). [In Russian] https://studfile.net/preview/4354159/page:16//
10. Karpov Yu. 2005 *System simulation modelling. Introduction to simulation with AnyLogic 5* [Имитационное моделирование систем. Введение в моделирование с AnyLogic 5]. BHV-Petersburg, pp. 400. [In Russian]
11. Parfionov Yu. 2011 *Mathematical apparatus selection for informational systems imitation models development* [Вибір математичного апарату при розробленні імітаційних моделей інформаційних систем]. Informational technologies in technical systems. Kharkiv: KhNEU. **Issue 3 (93),** pp. 69-71. [In Ukrainian]
12. Samofalov K., Korneichuk V., Romankevych A. and others 1987 *Applied theory of automatic digital devices* [Прикладная теория цифровых автоматов]. Kyiv: High school, pp. 375. [In Russian]
13. 1999 *Informational processes in modern networks. Protocols, standards, interfaces, models* [Информационные процессы в современных сетях. Протоколы, стандарты, интерфейсы, модели]. M.: Kudits-Obraz, pp. 256. [In Russian]
14. Tupkalo V. 2021 *Cyber secured informational systems management based on signature algebra mathematical apparatus use* [Розробка моделей кіберстійких інформаційних систем управління на основі використання математичного апарату сигнатурної алгебри]. V International sci.-pract. conf. «Education and industry quality management: experience, problems and prospects», theses report. Lviv: LA «Pyramid», pp. 186-187. [In Ukrainian]
15. Tupkalo V. M. 1994 *Theory fundamentals of digital systems signature control: a monograph* [Основы теории сигнатурного контроля цифровых систем: монография]. ME of Ukraine, pp. 324. [In Russian]
16. *Additional code* [Доповняльний код]. (Accessed 20.09.2022) [In Ukrainian] https://uk.wikipedia.org/wiki/Доповняльний_код
17. Kuznetsov A., Adelson-Velskiy G. 1980 *Discrete mathematics for an engineer* [Дискретная математика для инженера]. M.: Energy, pp. 344. [In Russian]
18. *Propertties and analytical representations of elementary Boolean functions of two variables* [Властивості й аналітичні подання елементарних булевих функцій від двох змінних]. (Accessed 20.06.2022) [In Ukrainian] https:// https://studfile.net/preview/3021634/page:17//