Journal of Theoretical and Applied Information Technology
15th December 2020. Vol.98. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPLEMENTATION OF INFORMATION SECURITY DEVICES IN EQUILIBRIUM CODES

I. E. LYUBUSHKINA, E. M. ZVEREV, A. V. SHARAMOK
National Research University of Electronic Technology (MIET), Shokina Square, 1, Zelenograd, Moscow, 124498, Russia
E-mail: lyubushkina.i.e@gmail.com

ABSTRACT

This article discusses the issue of data leakage via side channels in terms of development of radio masking. Formation of optimum masking for digital data processing devices has been substantiated on the basis of available results of electronic warfare theory. It is shown that the optimal masking interference will be formed when processing information in the inverse representation. Two methods of implementation of data processing devices in equilibrium codes have been considered. The first method in addition to leakage via side channels proposes duplication of data processing, which improves the reliability of data processing. The second method provides less opportunities to control the reliability of data processing but is more suitable for requirements of optimum deception. In order to substantiate the possibility of practical use of the proposed method, a mathematical model of computations in the inverse representation for Magma cryptographic algorithm has been developed. As further studies, it is planned to conduct experimental studies on the effectiveness of countering known types of attacks through side channels. Application of the considered methods is possible for development of trusted devices of cryptographic data protection with a high level of security. The approach to the problem of data protection against leakages through side channels considered in the study, the theoretical substantiation of the optimal masking interference and the developed mathematical model of the Magma cryptographic algorithm have been proposed by the authors for the first time.

Keywords: *Side Channels, Encryption Devices, Model of Computation, Magma Algorithm, Electronic Masking.*

1. INTRODUCTION

Development of trusted hard- and software platforms in protected embodiment is related with solutions to some specific problems. In such devices, in addition to implementation of various functional and trust requirements, it is required to provide protection against possible retrieval of open and sensitive information via the electromagnetic side channels (hereinafter referred to as the side channels) [1]. Herewith, sensitive information is any information, using which it would be possible to attack the embedded protection mechanism in hard- and software platform, for instance, cryptographic algorithms.

Possible retrieval of sensitive information is stipulated by existence in security devices (SD) of side channels: the channels of data transfer not stipulated by architecture of these devices and used not as standard channels of data transfer in actual SD (for instance, leakage of confidential data processed by encryption device via electromagnetic oscillations occurring during operation of computing devices) [1, 2]. Side channels appear as a consequence of certain physical effects occurring in equipment [1]. Herewith, the information from source via the transmission medium is transferred to receiver. At all stages of side channel existence, the information is presented in the form of certain physical carrier, physical field [1]. It should be noted that side channel attacks are quite real and can be implemented on modern computing facilities using relatively simple equipment [3].

This work is aimed at substantiation of computation model for cryptographic algorithm Magma, providing formation of optimum masking interference upon computations in SD. The novelty of the work is in the proposed substantiation of correct transformations by Magma algorithm upon computations in inverse form. This work proposes computation model allowing to protect encryption device, implementing Magma algorithm, against leakage via side channels.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. COUNTERMEASURE AGAINST SIDE CHANNELS

Conventional countermeasure against side channels is impact on side channel. Let us exemplify the impacts on side channels [1, p. 4]:

– on transmitter of side channel by reducing power of radiated signal by means of specialized hardware design;

– on transfer environment by increased attenuation in side channel by means of modification of transfer environment (shielding) or increase in the length of side channel (creation of controlled areas);

– on side channel receiver by creation of active jamming using noise devices.

The methods of impacts on side channel are widely applied upon development of data protection devices and in most cases provide the required performances. At the same time, such methods are characterized by fundamental restrictions, since they influence not information itself but physical data carriers of side channel. Let us exemplify some of these restrictions [1, p. 4]:

– occurrence of new methods of data retrieval from side channels (for instance, occurrence of new processing methods of received signals) leads to necessity to review sufficiency of properties of the applied protection methods;

– such methods are insufficient to block all side channels, which is stipulated by numerous physical effects and interactions between them, as well as by possible existence of unknown physical effects at the time of equipment development, hence, respective side channels created by them.

3. OPTIMUM MASKING SIGNAL

Let us consider protection against leakage via side channels by creation of active jamming. In order to analyze the optimum requirements to active jamming, let us consider the protection against data leakage via side channels in terms of theory of electronic warfare (EW) [2].

In the case of classic identification of EW problem, the following radio electronic tools are considered [4]: masked system comprised of transmitter of masked system and receiver of masked system, transmitter of active masking jamming and receiver of intelligence tools. In the case of protection against leakage via side channels, the masked system is comprised only of transmitter of the masked system, receiver of the masked system does not participate in radio electron conflict, which determines the specificity of radio masking problem upon leakage via side channels.

Figure 1 illustrates the flowchart of conflict interaction upon protection against leakage via side channels. In this case, the participants in conflict are SD comprised of transmitter of a signal with sensitive information (SI TX) and transmitter of electronic jamming (EJ TX), and receiver of intelligence tools (INT RX). SI TX transmits a signal with sensitive information and EJ TX transmits active jamming. INT RX attempts to receive sensitive signal on the background of active jamming. As mentioned above, transmittance of sensitive signal is stipulated not by necessity of transmit information but by physical properties of SD, that is, by the properties of physical effects applied in SD for implementation of data processing function.

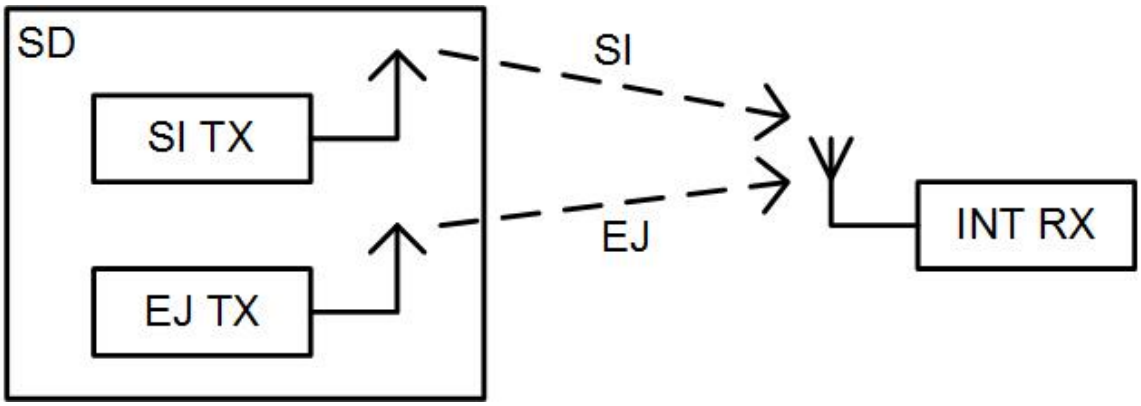

Figure 1: Flowchart of Conflict Interaction upon Protection Against TEMPEST

In terms of the problem, EW is considered as energy, structural, and information security of signals, in our case: signals of side channels. Under conditions of formulation of protection against side channels, it has no sense for SD to discuss energy security, it is required to consider structural security

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of signals of side channels. It is known that provision of structural security is possible by means of active masking.

According to [4], side channel for SD can be illustrated as follows (Figure 2).

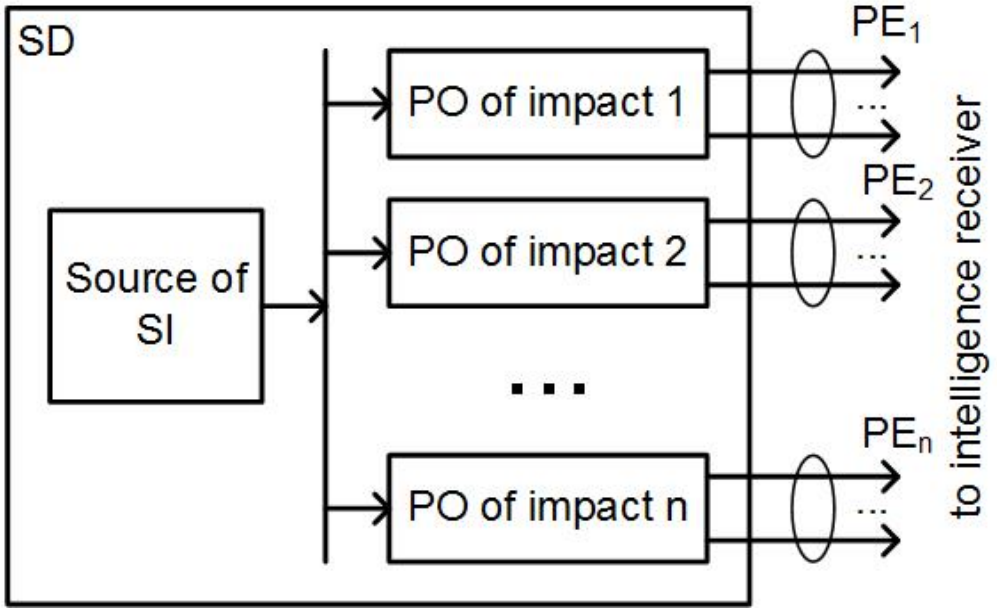

Figure 2: Flowchart of Channel Leakage via TEMPEST Medium

Herewith, SD can be characterized by both the existence of high number of physical objects (PO), on which the impact is exerted by the source of sensitive information (SI), and by cross couplings of results of physical effects (PE) on PO after impact on each other. Therefore, the number of possible channels of leakage of sensitive information can be very high.

If the methods of active radio masking are taken as basis, then the strategy of protection can be presented by the strategy of active radio masking in each identified side channel. At the same time, more promising is the strategy of active masking not of data carriers (their data parameters), but of information itself [5]. Indeed, it is possible to create a jammer, which provides active masking in each possible channel of data leakage.

From theoretical considerations of EW [4] it is known that structural security of signals can be achieved by minimization of posterior distribution of probabilities of protected signal by active masking, which is provided by simultaneous optimization of the following functions:

$$\frac{1}{N_0}\int_0^T \Pi(t,\lambda_n)^2 dt \to \max \quad (1);$$

$$\frac{1}{N_0}\int_0^T C(t,\lambda_c)\Pi(t,\lambda_n)dt \to \max \quad (2);$$

$$\frac{1}{N_0}\int_0^T x(t)\Pi(t,\lambda_n)dt \to \min \quad (3).$$

where $x(t)$ is the signal tracked by the intelligence receiver, $C(t,\lambda_c)$ is the signal of sensitive information with the parameters λ_c, $\Pi(t,\lambda_n)$ is the active jamming with the parameters λ_n, N_0 is the spectral density of noise power, T is the duration of signal tracking by intelligence receiver.

These conditions are interpreted in [4] as follows. Condition (1) assumes increase in jamming power, which is not always possible and justified. Condition (2) assumes maximization of mutual correlation between compromising signal and active jamming, which in the case of radio masking assumes maximum coincidence of active jamming with signal of sensitive information in terms of non-informative parameters for intelligence and maximum difference in terms of informative parameters. Condition (3) assumes minimization of mutual correlation between active jamming and signal tracked by intelligence.

The conditions (2) and (3) imply simulating

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

pattern of jamming and requirement of difficulty of spatial and time decomposition of masked signal and jamming.

Let us consider signals which are sources of side channels for SD. In modern digital devices (for instance, in programmable logical devices), information is presented in binary form and coded by voltage levels [6]. For CMOS devices with 5 V logics the logical zero corresponds to low level (voltage from 0.0 V to 1.5 V), the logical one corresponds to high level (voltage from 3.5 V to 5.0 V) [6]. Thus, it is possible to state that the following parameters of signal in side channels are informative for intelligence: voltage level (corresponds to logical zero or logical one) and transitions from one voltage level to another (transition from logical zero level to logical one level and transition from logical one level to logical zero level).

Let us denote the informative parameters of signal with sensitive information as follows: λ_0 is the signal with logical level 0; λ_1 is the signal of transition from logical level 0 to logical level 1; λ_2 is the signal with logical level 1; λ_3 is the signal of transition from logical level 1 to logical level 0. Then, the active jamming is optimum when it complies with Eqs. (1), (2), (3), and λ_i, comprising informative parameter $\lambda_{(i+2)mod4}$, with existence of informative parameter in the signal with sensitive informayion. Let us synthesize an optimum jamming for SD satisfying these requirements. The jamming will be comprised of formation of parameter λ_2 in active jamming upon existence in informative signal of parameter λ_0, formation of parameter λ_0 in active jamming upon existence in informative signal of parameter λ_2, formation of parameter λ_1 in active jamming upon existence in informative signal of parameter λ_3, formation of parameter λ_3 in active jamming upon existence in informative signal of parameter λ_1. That is, if an informative signal is a certain sequence of binary values B, then the active jamming should be comprised of logical inversion of the sequence B. The requirement of difficulty of spatial and time decomposition of masked signal and active jamming implies the necessity of time synchronous transmittance and processing of masked signal and active jamming, as well as the maximum possible mutual positioning of signal sources, for instance, conductors in SD.

For intelligence receiver such jamming provides probability of error by the symbol P_{err}=0.5 [7], which confirms its optimality. It is mentioned in [7] that the case of jamming synchronous with but inverse to signal with the power level equaling to that of masked signal is "rather artificial" in terms of classical problem of EW. As follows from this article, application of such jamming in SD is a reasonable and efficient protection against data leakage via side channels.

4. DEVELOPMENT OF SECURITY DEVICES

Upon implementation of the considered protection against leakage via side channels in actual devices, two approaches are possible:

- development of two parallel operating flowcharts (units or devices), one of which operates in direct representation, and the other synchronously operates in inverse representation (the first approach);

- development of single device operating in equilibrium code (the second approach).

The two approaches are compared in Figure 3.

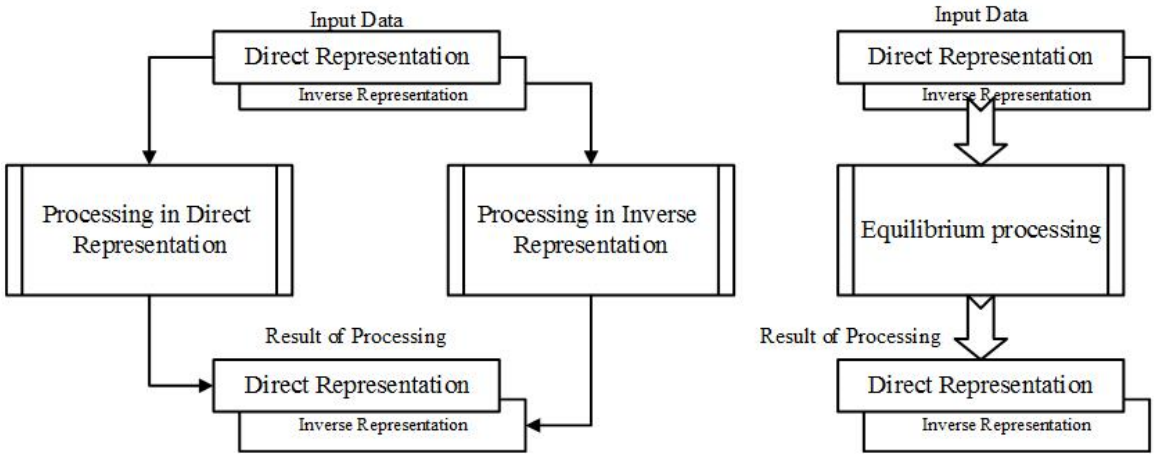

Figure 3: Comparison of Two Approaches to Implementation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Let us consider the features of both approaches. Each of the considered approaches has its advantages and disadvantages. Thus, for instance, the second approach due to concentrated implementation in one device provides difficulty of spatial decomposition of signals of side radiations for intelligence, which according to [2] improves protection efficiency. Moreover, implementation in one device simplifies synchronous processing in direct and inverse representation [6], which also improves protection against leakage via side channels [4]. However, the first approach makes it possible simultaneously with protection against leakage via side channels to perform duplicated processing with subsequent control of results of two independent computations, which is an obligatory condition upon implementation of encryption devices with high level of security and trust [8].

5. MATHEMATICAL MODEL OF INVERSE COMPUTATIONS

The possibility of inverse computations is substantiated in [9]. Then, let us describe the mathematical model of operation of two parallel flowcharts: modulo 2^n addition and modulo $2^{32} - 1$ addition on the basis of approach in [9].

In order to eliminate ambiguous interpretation of further consideration, let us introduce some notions from the modular arithmetic [10]. Let us denote direct representation of n-bit value as a and its inverse n-bit representation as $\bar{a}$ in the discussed in [2, p. 43] sense. Let us assign the symbol Z_{2^n} to the ring of all remainders (mod 2^n residuals) obtained by division of integers by 2^n. The set Z_{2^n} is comprised of integers: $0 \leq a < 2^n$. It is obvious that the numbers of this set are uniquely represented by binary code of the length n, Z_{2^n} is the ring. Let us consider additive iteration of this ring:

$$\forall\, a, b \in Z_{2^n}$$
$$a \boxplus b := |a + b|_{2^n},$$

where the right-hand part is the binary number equaling to the remainder after division of binary sum of a and b by 2^n. The remainder of division of integer $x \in Z$ by 2^n is denoted by the symbol $|x|_{2^n}$.

Therefore, the Euclid's theorem [10] for this case is as follows:

$$\forall x \in Z, x = q \cdot 2^n + |x|_{2^n}$$

Here q is the incomplete quotient of division of x by 2^n, $q := \left[\frac{x}{2^n}\right]$. Respectively, $|x|_{2^n}$ is referred to as the remainder of division of x by 2^n.

The important properties used below are as follows:

$$\forall\, x \in Z_{2^n}, |x|_{2^n} = x \qquad (4)$$
$$\forall x, y \in Z, |x + y|_{2^n} = ||x|_{2^n} + |y|_{2^n}|_{2^n} \qquad (5)$$
$$\forall\, x \in Z_{2^n}, \bar{x} := 2^n - 1 - x,$$

Obviously,

$$\bar{x} \in Z_{2^n} \text{ and } \forall\, x \in Z_{2^n}$$
$$x + \bar{x} = 2^n - 1 \qquad (6)$$

6. INVERSE MODULO 2^N ADDITION

On the basis of the aforementioned, let us consider $\overline{\sum}_{2^n}$ adder operating with inverse representation of numbers. To be more exact, if the adder for direct representation of $\sum_{2^n}$ executes operations $|a + b|_{2^n}$, then the adder for inverse representation executes the following operation: the operands $\bar{a}$, $\bar{b}$, are fed to the input, and the result at the output is $\overline{|a + b|_{2^n}}$.

Let $a, b \in Z_{2^n}$. Taking into account Eq. (6):

$$\overline{|a + b|_{2^n}} = 2^n - 1 - |a + b|_{2^n} \qquad (7)$$

According to the Euclid's theorem:

$$|a + b|_{2^n} = a + b - \xi_0 \cdot 2^n,$$

where $\xi_0 = \left[\frac{a+b}{2^n}\right]$.

Substituting the latter identity into Eq. (7), we have:

$$\overline{|a + b|_{2^n}} = 2^n - 1 - (a + b) + \xi_0 \cdot 2^n \qquad (8)$$

Then, using Eq. (6), we convert the right-hand part of Eq. (8) as follows:

$$\overline{|a + b|_{2^n}} = \bar{a} + \bar{b} + \xi_0\, 2^n - 2^n + 1$$

Determining the remainder of division of the latter identity (left and right) by 2^n we have:

$$\left|\overline{|a + b|_{2^n}}\right|_{2^n} = \left|\bar{a} + \bar{b} + 1\right|_{2^n}$$

However, since:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$\overline{|a+b|_{2^n}} \in Z_{2^n},$$

then according to Eq. (1):

$$\left|\overline{|a+b|_{2^n}}\right|_{2^n} = \overline{|a+b|_{2^n}}$$

Thus, the following identity is obtained:

$$\left|\bar{a}+\bar{b}+1\right|_{2^n} = \overline{|a+b|_{2^n}} \qquad (9)$$

which determines the adder operation in inverse mode:

$$\sum_{2^n} + 1(\mathrm{mod} 2^n) \rightarrow \overline{|a+b|_2}.$$

Therefore, the $\mathrm{mod}\, 2^n$ adder operating with inverse representation should have at input, in addition to the arguments $\bar{a}$ and $\bar{b}$, the argument in the form of constant equaling to 1 in the least significant position of the adder.

7. INVERSE MODULO 2^{32}– 1 ADDITION

Now let us consider the logics of $2^{32} - 1$ adder using the notations introduced above. Let we have two operands: $a, b \in Z_{2^n}$. It is required to determine the sum in inverse representation for $|a+b|_{2^n-1}$

According to Eq. (6):

$$a + b = 2(2^n - 1) - (\bar{a} + \bar{b})$$

or

$$|a+b|_{2^n-1} = \left|-(\bar{a}+\bar{b})\right|_{2^n-1}$$

However,

$$\left|-(\bar{a}+\bar{b})\right|_{2^n-1} = \left|2^n - 1 - |\bar{a}+\bar{b}|_{2^n-1}\right|_{2^n-1}$$

Hence,

$$\overline{|a+b|_{2^n-1}} = \left|\bar{a}+\bar{b}\right|_{2^n-1}$$

It means that in the $\sum_{2^n-1}$ adder correct adding is executed of values presented in inverse form. Thus, if at its inputs the inverse values are fed, $\bar{a}$ and $\bar{b}$, then the $\sum_{2^n-1}$ adder outputs correct inverse sum $\overline{|a+b|_{2^n-1}}$.

8. INVERSE MODULO 2 ADDITION

Let us consider the operation logics of modulo 2 adder using the table representation [6].

Table 1: Modulo 2 Addition

a	b	$a \oplus b$	$\bar{a}$	$\bar{b}$	$\bar{a} \oplus \bar{b}$
a	0	a	$\bar{a}$	1	a
0	b	b	1	$\bar{b}$	b
a	1	$\bar{a}$	$\bar{a}$	0	$\bar{a}$
1	b	$\bar{b}$	0	$\bar{b}$	$\bar{b}$

It can be seen in the table that the result of modulo 2 addition of direct and inverse data coincides. That is:

$$\bar{\bar{a}} \oplus \bar{\bar{b}} = a \oplus b = \bar{a} \oplus \bar{b}.$$

If we assume $\bar{a} \oplus \bar{b} = x$, and $x \oplus 1 = \bar{x}$, then:

$$a \oplus b \oplus 1 = \overline{\bar{a} + \bar{b}}.$$

From the latter it can be seen that mutually inverse representation of results of modulo 2 adders can be obtained either by inversion of output result, or in the case when the adder ends with register flowchart, where data can be retrieved from its inverse branch of trigger flowcharts.

9. INVERSE IMPLEMENTATION OF SINGLE BLOCK OPERATION OF MAGMA CRYPTOGRAPHIC ALGORITHM

In order to implement parallel operating flowcharts of cryptographic transformation in equilibrium code, implementability is required of inverse computations for operations constituting cryptographic transformation. The transformation should be executed so that to retain isomorphism between transformations in direct and inverse representations, that is, if for input data Eq. (6) is valid, then this ratio should be valid for output data of the transformation. Let us demonstrate that the block cipher Magma, is characterized by such properties [11].

Input data of transformation. Data in inverse representation, conforming Eq. (6) for respective data in direct representation, should be fed to the input of inverse variant.

$a_{\text{inv.}} = \overline{a_{dir.}}$, where a is the input data.

Internal data of transformation. The internal data of the algorithm are the key and the values of π_i' substitutions. Taking into account

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

execution of Eq. (6) in inverse variant of the algorithm, the internal data are transformed as follows:

$K_{inv} = \overline{K_{dir}}$, where K is the key of cryptographic transformation.

The content of each array of π_i' substitutions varies according to the equation: $\pi[\bar{i}] = \overline{\pi[i]}$, that is, in a cell with inverse address the inverse content of the cell with direct address is fed. The inverse values of substitution tables of Magma algorithm from [11] are summarized in Table 2.

Table 2: Inverse Table of Magma Algorithm Substitution

π[0]	π[1]	π[2]	π[3]	π[4]	π[5]	π[6]	π[7]
0×E	0×0	0×F	0×4	0×3	0×F	0×7	0×D
0×0	0×15	0×9	0×6	0×D	0×1	0×1	0×4
0×C	0×2	0×6	0×1	0×B	0×C	0×D	0×3
0×F	0×4	0×3	0×C	0×4	0×B	0×A	0×6
0×8	0×8	0×B	0×A	0×1	0×E	0×9	0×9
0×2	0×B	0×8	0×5	0×C	0×7	0×6	0×5
0×7	0×1	0×E	0×F	0×6	0×8	0×E	0×0
0×1	0×E	0×1	0×8	0×F	0×4	0×3	0×B
0×6	0×3	0×2	0×9	0×2	0×5	0×0	0×C
0×4	0×A	0×5	0×0	0×9	0×3	0×B	0×7
0×A	0×5	0×0	0×B	0×E	0×D	0×4	0×A
0×5	0×6	0×D	0×2	0×7	0×6	0×F	0×F
0×D	0×C	0×7	0×E	0×5	0×9	0×2	0×2
0×9	0×D	0×A	0×D	0×A	0×0	0×5	0×1
0×B	0×7	0×C	0×7	0×0	0×2	0×C	0×8
0×3	0×9	0×4	0×3	0×8	0×A	0×8	0×E

Output data of transformation are the inverse values of transformation results.

While meeting the two aforementioned rules of inverse mathematics, the basic encryption algorithm in inverse form is illustrated in Figure 4.

Operations in inverse representations (modulo 2^{32}-1 addition and modulo 2 addition considered above) are highlighted in grey, they are not present in the basic Magma algorithm. Herewith, the K key is presented in inverse form, and inverted table of substitutions π_i' is used, the data in inverse form are delivered to input.

Since the inverse transformation mode includes additional operations, synchronization of transformations in direct and inverse representations should be performed here, which would provide conformity with the requirements in [4] and optimum protection against leakage via side channels. Synchronization can be performed by additional dummy operations in direct representation.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

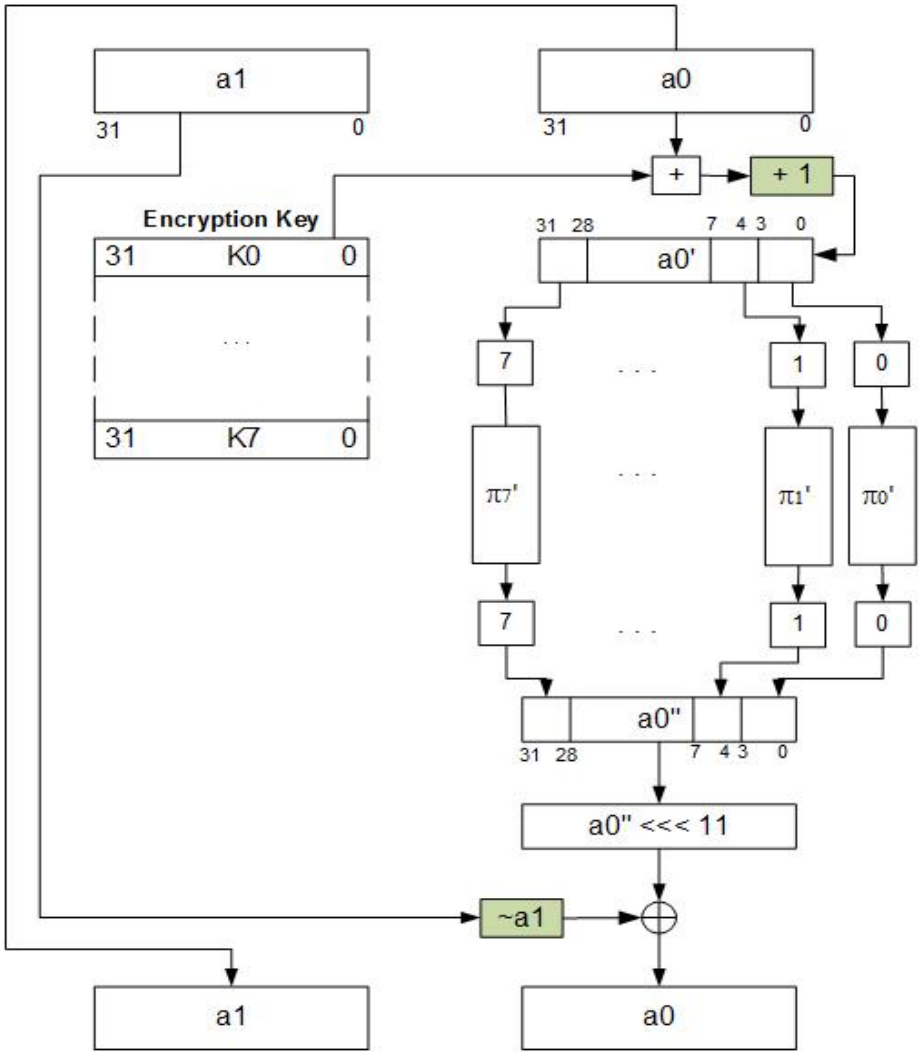

Figure 4: Inverted Single Block Operation

10. IMPLEMENTATION OF EQUILIBRIUM PROCESSING IN THE FORM OF SINGLE DEVICE

While implementing equilibrium processing in the single device, it is required to stipulate coding of 0 and 1. Let us assume that 0 corresponds to the equilibrium code 01, 1 corresponds to the equilibrium code 10. In this case, the truth table of modulo 2 addition will be presented in the form of Table 3.

Table 3: Modulo 2 Addition in Equilibrium Code

a	*b*	*a*⊕b
01	01	01
01	10	10
10	01	10
10	10	01

More interesting is the implementation of adder in equilibrium code. Let us consider binary full adder [6]. Operation of full adder is described by the following equations:

$$s = a \otimes b \otimes c_{-1} = a \cdot \overline{b} \cdot \overline{c}_{-1} + \overline{a} \cdot b \cdot \overline{c}_{-1} + \overline{a} \cdot \overline{b} \cdot c_{-1} + a \cdot b \cdot c_{-1}. \quad (10)$$

$$c = a \cdot b + a \cdot c_{-1} + b \cdot c_{-1}. \quad (11)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

where s is the least significant bit of adding; a, b are the first and the second operands, respectively; c_{-1} is the third operand (transfer from the previous position); c is the high bit of the adding (transfer to the next position); $\otimes$ is the modulo 2 addition; $\cdot$, $+$ are the conjunction and disjunction operations, respectively; $\bar{}$ is the inversion operation.

It is possible to demonstrate that binary full adder operates correctly with inverse representation of numbers. For inverse bit of adding we demonstrate it by means of complete induction method [6], with this aim we will arrange the truth table for Eq. (10) and demonstrate that it is inverse for direct representation upon operation with inverse values:

Table 4: Validity for Sum in Equilibrium Code

a		b		c_{-1}		s	
0	1	0	1	0	1	0	1
0	1	0	1	1	0	1	0
0	1	1	0	0	1	1	0
0	1	1	0	1	0	0	1
1	0	0	1	0	1	1	0
1	0	0	1	1	0	0	1
1	0	1	0	0	1	0	1
1	0	1	0	1	0	1	0

In order to substantiate correct operation of full adder with inverse carry bit, let us apply the method of reduction of Boolean expressions. With this aim, let us substitute inverse values of equilibrium code into Eq. (11):

$$c^i = \bar{a}\cdot\bar{b} + \bar{a}\cdot\bar{c}_{-1} + \bar{b}\cdot\bar{c}_{-1} = \overline{(a+b)} + \overline{(a+c_{-1})} + \overline{(b+c_{-1})} =$$

$$= \overline{(a+b)\cdot(a+c_{-1})\cdot(b+c_{-1})} = \left| \begin{array}{l} expanding\ the\ brackets\ and\ reducing\ the\ terms \\ in\ accordance\ with\ Boolean\ algebra \\ we\ obtain\ the\ following \end{array} \right| =$$

$$= \overline{a\cdot b + a\cdot c_{-1} + b\cdot c_{-1}} = \overline{c^d}.$$

From the above considerations it follows that the full adder correctly processes inverse values of equilibrium code, hence, the full adder for equilibrium code can be presented as two synchronously operating full adders, one of which processes direct discharges of equilibrium code and the other processes inverse discharges of equilibrium code (Figure 5).

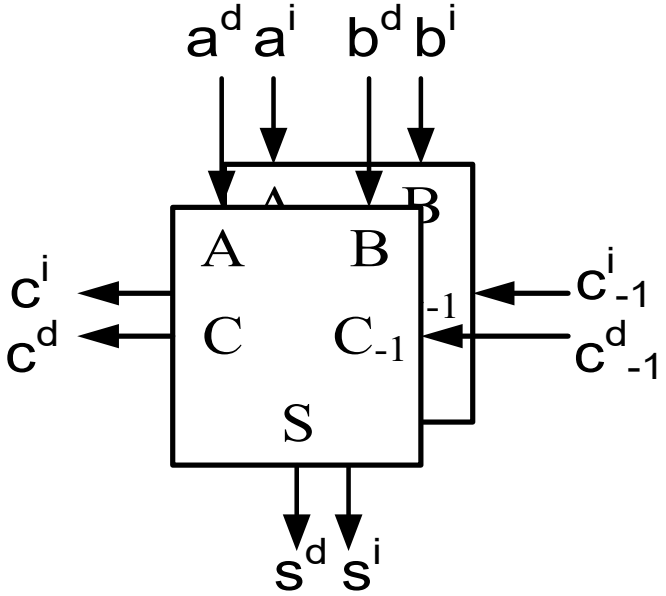

Figure 5. Full Adder in Equilibrium Code

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In Figure 5 the direct discharges of equilibrium code are denoted by the index **d**, the inverse discharges of equilibrium code are denoted by the index **i**.

11. DISCUSSION

The research of protection against data leakage via side channels and side channel attacks has been performed over the last 30 years. During this time, a number of methods countering these attacks and being effective in individual cases have been proposed [12]. Analysis of research in this area has allowed identifying the following main methods of countering side channel attacks. Introduction of randomness into the processed data and into the process of their processing [13, 14]. A special case of introducing randomness is masking the processed data with random data [5, 12, 15, 16]. The main disadvantage of masking is its nonarithmeticity, i.e. the inability to perform all the necessary arithmetic conversions with masked data [5]. At the same time, it is possible to perform separate arithmetic operations with masked data [5, 16]. The lack of arithmeticity leads to the need to remove masks when performing certain operations [16], which entails a decrease in protection against attacks through side channels and a decrease in the speed of cryptographic operations. The use of secret sharing method and multilateral computation [12, 17]. Secret sharing applied for protection against side channel leakages is considered to be an effective method; however, unlike the previous method, it requires for hardware implementation and leads to at least a threefold increase in hardware resources [17]. The closest method to the one considered in this study is the implementation of devices with dual-rail logic [18]. At the time of the first studies on the use of devices with dual-rail logic, it was believed that this approach was promising for implementation in microelectronic devices protected against side channel attacks [18]. It should be noted that the devices with dual-rail logic were used mainly for protection against a Differential Power Analysis (DPA) attack [18]. Recent studies have shown that there is no significant advantage of using devices with dual-rail logic over the traditional CMOS microelectronic devices in terms of economic efficiency of protection [19]. The method proposed in this study allows for an additional analysis and improvement of the dual-rail logic application in terms of data protection against leakage through electromagnetic radiation channels, as well as has a significant advantage over the devices with dual-rail logic, since it allows the duplicated information processing in two devices (e.g. cryptographic algorithms implementation in two duplicating FPGA chips). In some cases, this does not lead to an increase in the cost of cryptographic devices and, accordingly, to a decrease in the economic efficiency of protection, since the implementation of duplicated processing is a mandatory requirement for cryptographic devices with a high level of security [8].

12. CONCLUSION

The protection against data leakage via side channels considered in this article is theoretically substantiated and is sometimes more efficient in comparison with conventional methods. Within the framework of this article, it has been proposed to consider the issue of protection against data leakage via side channels from the point of view of the theory of electronic warfare, which allowed formulating requirements for the optimal masking interference. Based on these requirements, it has been shown that the optimal masking interference will be formed when processing information in the inverse representation. In order to substantiate the possibility of practical implementation of the proposed method, a mathematical model of computations in inverse representation for the Magma cryptographic algorithm has been developed. The research analysis has shown that the approach to the problem of protection against data leakage through side channels, the theoretical substantiation of the optimal interference and the developed mathematical model of the Magma cryptographic algorithm were proposed by the authors for the first time. As further research, it is advisable to outline the development of similar mathematical models for other widely used and promising cryptographic algorithms, to conduct experimental research on the effectiveness of countering devices developed in accordance with the proposed methodology, known types of side channel attacks. The mathematical models based on the considered method are proposed for application in trusted hard- and software of data protection developed by Trusted Sensor Systems (MIET: National Research University of Electronic Technology). The prerequisites to implementation of the considered method are development of microelectronic production technologies of custom specialized computing devices. In this regard, application of the method is less expensive and more cost efficient upon implementation of trusted microelectronic devices.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ACKNOWLEDGMENTS

This article was performed in the framework of the program titled Trusted sensor systems (Agreement No. 009/20 dated April 10, 2020) with financial support by the Ministry of Communications and Mass Media of the Russian Federation and AO RVC. Project ID: 0000000007119P190002.

REFRENCES:

[1] A.N. Sobolev, V. M. Kirillov, "Fizicheskie osnovy tekhnicheskikh sredstv obespecheniya informatsionnoi bezopasnosti" ["Physical foundations of technical tools protecting information safety"], Guidebook, Gelios ARV, Moscow, 2004.

[2] A.V. Sharamok, "Obespechenie strukturnoi skrytnosti informativnykh signalov pobochnykh elektromagnitnykh izluchenii i navodok" ["Provision of structural security of information signals of spurious electromagnetic radiations and pickups"], *Spetsial'naya tekhnika*, Vol. 3, 2011, pp. 30-33.

[3] D. Genkin, I. Pipman, E. Tromer, "Get your hands off my laptop: physical side-channel key-extraction attacks on PCs", J. Cryptogr. Eng., Vol. 5, 2015, pp. 95-112. https://doi.org/10.1007/s13389-015-0100-7

[4] V.P. Demin, A.I. Kupriyanov, A.V. Sakharov, "Radioelektronnaya razvedka i radiomaskirovka" ["Electronic intelligence and radio deception"], MAI, Moscow, 1997.

[5] V.M. Amerbaev, D.V. Tel'pukhov, A.V. Sharamok, "Sposob skrytogo slozheniya i osobennosti ego realizatsii" ["Concealed summation and peculiarities of its implementation"], *Izvestiya vuzov: Elektronika*, Vol. 3, No. 77, 2009, pp. 26-32.

[6] J. F. Wakerly. "Digital Design: Principles and Practices", Vol 1, Prentice Hall, 2000.

[7] V.M. Garbuz, A.S. Kislitsin, A.I. Kupriyanov, E.M. Sukharev, "Optimal'naya strategiya zashchity ot perekhvata signala tsifrovykh radiotelemetricheskikh sistem peredachi dannykh, Modeli tekhnicheskikh razvedok i ugroz bezopasnosti informatsii" ["Optimum strategy of protection against signal interception of radio telemetric digital data transfer systems. Models of technical intelligences and hazards of data safety"], Collective Monograph, Book 3, Radiotekhnika, Moscow, 2003.

[8] A.V. Sharamok, "Apparatnaya realizatsiya GOST-28147-89 dlya prozrachnogo shifrovaniya potokov dannykh" ["Hardware implementation of State standard GOST-28147-89 for transparent encryption of data flows"], RusKripto'2013, Moscow, 2013.

[9] V. M. Amerbaev, E. M. Zverev, N. O. Kutsepalov, I. E. Lyubushkina, "Sobstvennaya bezopasnost' informatsionnykh kriptoshifratorov i metody eyo realizatsii" ["Inherent security of data encryptors and methods of its implementation"], *Sozidateli otechestvennoi elektroniki*, Issue 5, Tekhnosfera, Moscow, 2012, pp. 394-426.

[10] I.M. Vinogradov, "Osnovy teorii chisel" ["Foundations of theory of numbers"], Gosudarstvennoe izdanie tekhniko-teoreticheskoi literatury, Moscow 1953.

[11] "State standard GOST 34.12-2018. Information technology. Cryptographic data security. Block ciphers".

[12] B. Robisson, H.L. Bouder, "Physical functions: the common factor of side-channel and fault attacks?", *J. Cryptogr. Eng.*, Vol. 6, 2016, pp. 217-227. https://doi.org/10.1007/s13389-015-0111-4

[13] W. He, E. de la Torre, T. Riesgo, "An Interleaved EPE-Immune PA-DPL Structure for Resisting Concentrated EM Side Channel Attacks on FPGA Implementation". In: Schindler W., Huss S.A. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2012. Lecture Notes in Computer Science, Vol. 7275. Springer, Berlin, Heidelberg, 2012. https://doi.org/10.1007/978-3-642-29912-4_4

[14] P. Sasdrich, O. Mischke, A. Moradi, T. Güneysu, "Side-Channel Protection by Randomizing Look-Up Tables on Reconfigurable Hardware". In: Mangard S., Poschmann A. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2015. Lecture Notes in Computer Science, Vol. 9064. Springer, Cham, 2015. https://doi.org/10.1007/978-3-319-21476-4_7

[15] P.K. Vadnala, J. Großschädl, "Faster Mask Conversion with Lookup Tables". In: Mangard S., Poschmann A. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2015. Lecture Notes in Computer Science, Vol. 9064. Springer, Cham, 2015. https://doi.org/10.1007/978-3-319-21476-4_14

[16] D. Goudarzi, A. Journault, M. Rivain, F.X. Standaert, "Secure Multiplication for Bitslice Higher-Order Masking: Optimisation and Comparison". In: Fan J., Gierlichs B. (eds)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Constructive Side-Channel Analysis and Secure Design. COSADE 2018. Lecture Notes in Computer Science, vol 10815. Springer, Cham, 2018. https://doi.org/10.1007/978-3-319-89641-0_1

[17] S. Kutzner, P.H. Nguyen, A. Poschmann, H. Wang, "On 3-Share Threshold Implementations for 4-Bit S-boxes". In: Prouff E. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2013. Lecture Notes in Computer Science, Vol. 7864. Springer, Berlin, Heidelberg, 2013. https://doi.org/10.1007/978-3-642-40026-1_7

[18] D. Suzuki, M. Saeki, "Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style". In: Goubin L., Matsui M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, Vol. 4249. Springer, Berlin, Heidelberg, 2006. https://doi.org/10.1007/11894063_21

[19] K. Nawaz, D. Kamel, F.X. Standaert, D. Flandre, "Scaling Trends for Dual-Rail Logic Styles Against Side-Channel Attacks: A Case-Study". In: Guilley S. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2017. Lecture Notes in Computer Science, Vol. 10348. Springer, Cham, 2017. https://doi.org/10.1007/978-3-319-64647-3_2