Hardware Implementation of Data Transmission Control based on Boolean Transformation

Dr. N.G BARDIS [1], Dr. E.G BARDIS [2], Dr. A.P. MARKOVSKYY [3], C. ECONOMOU [4]

[1] Adjunct Assistant Professor
Department of Automation
Technological Education Institute of Halkis
34400 Psahna, Halkis, Evia, Greece

Research Associate
Hellenic Naval Academy
Military Inst. of University Education / Hellenic Naval Academy
http://www.rgcds.org

[2]Hellenic Ministry of Public Order,
4, P. Kanelopoulou,
10177 Athens
GREECE

[3]Department of Computer Engineering
National Technical University of Ukraine
37, Peremohy, pr. Kiev 252056, KPI 2003,
UKRAINE

[4]Lecturer
Department of Computer Science, IST Studies
72, Pireos str, Moschato
183 46, Athens, Greece

Abstract: -In this paper an analysis and realization of Data Transmission Control based on Boolean Transformation for increasing the reliability of checksum and echoplex error detection has been proposed. Such transformations are used to amplify single errors and decrease the probability of undetected errors. The efficiency of the Boolean transformations in checksum and echoplex error detection schemes are compared with the known and ordinary methods of checksum, echoplex and CRC error detection schemes. Design and hardware implementation of the Data Transmission Control based on Boolean Transformation approach is presented.

Key words:- Error Detection, checksum, echoplex, SAC functions, Error Control Systems.

1 INTRODUCTION

Error detection is the process of monitoring the received data and determining when a transmission error has occurred. The problem of error detection effectiveness is important and actual for many data transmission systems.

From the practical utilization standpoint it makes sense to consider the following error detecting methods criterions:

- Error detecting reliability
- Additional checking information value
- Checking operation time
- Error response time

For the majority of the practical applications, the most effective, is the Cyclic Redundancy Checking (CRC). CRC is most reliable, but its implementation is sequential in principle. Peterson and Brown's scheme which is usually used for CRC hardware implementation is serial by bits so that CRC computation speed is limited in principle. Apart from this, as all error detecting methods in data blocks, CRC has high error response time.

These factors stimulated researches for increasing the reliability of alternative error detecting methods,

which ensure high checking operation speed and low error response time. In particular, the highest checking operation speed is achieved using checksum while the Echoplex method has the lowest error response time.

Checksum is one of the most widely utilized in practice means of detecting errors that appear when blocks of codes are being transfered in the channel [4]. In comparison to CRC, the checksum implementation is simple and requires significantly less time.The most important disadvantage of checksum error detection is in its deficient level of probability in detecting multiple errors due to their mutual masking.

Echoplex is a widely used method of error detection in duplex channels. Utilization of this error detection method is foreseen by a number of data transmission protocols, in particular by the widely used standard ITU-T ISDN [4].

Comparing it with checksum and CRC, echoplex has some important advantages. In particular,

- Echoplex ensures the quick reaction of the data-transmission system in case an error appears, making it effective for error detection in real time systems;
- Echoplex ensures a significantly high probability of error detection because checking is done in one cycle of transmission upon code which is substantially less in comparison with other methods, which detect errors in lengthy data blocks;

Echoplex has some disadvantages, most important of which are: the possibility of masking a forward transmission error by a reverse transmission error and the possibility of a false error detection, if the error appears at the reverse transfer of code (echo-code).

Nowadays the dynamic increase in the amount of information transferred, relative to speed, results in a decrease of the reliability in transferring data. As a result, the important problem of checksum and echoplex utilization is increasing error detection reliability**.**

2 ANALYSIS OF CHECKSUM AND ECHOPLEX ERROR DETECTION RELIABILITY

The main reason for the mentioned above checksum and echoplex disadvantages is the low effectiveness of coding the errors that are prevailed in practice. In practice, one or two types of errors are dominative, according to the characteristics of data transmission channel.

In many cases the appearance of a single error is prevalent. So, we shall cover the approach to increasing checksum and echoplex reliability for the case when the mentioned above type of error is dominative.

In such a case, it can be assumed that in one code, no more than one error appears and the multi errors appear in different codes of block. For the error appearance, we suppose the binomial error model. We can turn our attention to the fact that the probabilities p of the erroneous transmission of one bit is very small and the length n of the transmitted code is also small (n<=32). Thus, we can suppose that only a single error appears during the transmission of n-bit codes.

Suppose, that a data block contains k codes: D_1, D_2,…,D_k, each having a length of n bits. Traditionally checksum S of the data block is formed in such a way so that each bit of checksum is the XOR of the same bits in all codes of the block: $S = D_1 \oplus D_2 \oplus ... \oplus D_k$. In practice, the amount of errors appearing in the transmitted block does not exceed 3-4 erroneous bits. Therefore, it is justified to analyze the probability P_{2c} of dual undetected erors and the probability P_{4c} of fourfold undetected errors.

With the traditional formation of checksum, the errors will not be detected if a pair of them occur at the same bit positions of the transmitted codes. In this case, there is a mutual masking of errors in checksum code.

It has been easy to show that:

$$P_{2c} = \frac{1}{n} \tag{1}$$

$$\text{and } P_{4c} = \frac{2}{n^2} + \frac{1}{n^3} \tag{2}$$

The single error which appears in forward transmission will not be detected by echoplex, if it is masked by a single error which appears during reverse data transmission in the same bit position. The probability P_e of such situation is determined by the product of the probability of the error appearing during forward transmission at any position in the n bits of the code, with the probability of the error appearing in a fixed bit position during the reverse transmission.

$$P_e = \binom{n}{1} \cdot p \cdot (1-p)^{n-1} \cdot p \cdot (1-p)^{n-1} = \\ = n \cdot p^2 \cdot (1-p)^{2\cdot(n-1)} \tag{3}$$

The deficient level of probability checksum and echoplex single error detection was produced by noneffetiveness of errors coding.

Suppose that code D is transmitted and a single error appears in bit position k. Denote as $\Delta(D,k)$ – n-bit length code of checkcode change which is a result of such transmission error. The total possible single errors number is defined as the possible number of pairs <D,k> and is equal $n \cdot 2^n$. At the same time, the number of different codes $\Delta(D,k)$ in usual checksum or echoplex is equal n, because code $\Delta(D,k)$ does not depend on D and is the same for all possible 2^n codes X. It is clear that such error coding is not effective and results in a low level checksum and echoplex reliability.

It is sense that checksum and echoplex reliability can be increased by using special functional transformations which allow to increase the number of possible codes $\Delta(D,k)$ for the single error case. We propose to utilize a system of orthogonal Boolean functions which satisfy Strict Avalanche Criterion (SAC) as such function transformation.

3 UTILIZATION OF AVALANCHE TRANSFORMATION IN CHECKSUM AND ECHOPLEX ERROR CONTROL

To decrease the probability of error masking in checksum and echoplex error detecting schemes we propose to use Avalanche Transformations. Such a transformation plays the role of a single error amplifier and it can be realized as a system of orthogonal Boolean functions which satisfy the Strict Avalanche Criterion (SAC).

Usually these types of Boolean transformations are used in cryptographic algorithms and their design methods have been developed in [1,2].

A Boolean function $f(x_1,\ldots,x_n)$ defined on a set Z of all possible 2^n n-tuples of n variables, satisfies the SAC, if a complement of a single incoming n-tuple data bit changes the output of the Boolean function with probability 0.5:

$$\forall j \in \{1,...,n\}:$$

$$\sum_{x_1,\ldots,x_n \in Z} (f(x_1,...,x_j,...,x_n) \oplus f(x_1,...,\overline{x_j},...,x_n)) = 2^{n-1} \quad (4)$$

If one of the n inputs of the avalanche transformation is changed then half of its outputs will be changed. This means, that there is an ”avalanche amplifier” which by changing one of the n-tuple incoming data bit transforms half of the outputs. Because every function of this system satisfies the Avalanche Criterion, these transformations are called “avalanche”.

Let’s denote with F(D), the Boolean orthogonal avalanche transformation on the n-bits code D. The length of the transformed code R=F(D) is n bits long, as well. The orthogonality of the F(D) transformation indicates the one-to-one correspondence of codes D and R. The avalanche properties of the F(D) transformation indicate that if one bit of the input code D is changed then, on average, n/2 bits of the output code R=F(D) will be changed also.

In the [6] a new scheme for the transmitter’s checksum was introdused by Leros A where when a single error appears, then n/2 bits of the modified checksum will change. If a second error appears then another n/2 bits of the modified checksum will change. It is clear that the probability of the masking interaction of n/2 erroneous bit pairs is less than the probability of the masking interaction of a single bit pair.

The proposed control scheme of utilizing the avalanche transformation in the checksum is shown in Fig.1

In the [6] a new aproach for the echoplex error detection was introdused by Bardis N.G. The proposed scheme of utilizing avalanche transformation in echoplex error detection is shown in Fig. 2.

The transmitter executes the avalanche transformation $F(D_s)$ on code D_s which is sent to the channel. The transformed code $F(D_s)$ is stored in the transmiter’s memory. The receiver, gets the code D_r from the channel output, it executes the avalanche transformation on the code D_r and the result $F(D_r)$ is sent back to the echo channel. The transmitter receives the code R_e from echo channel and compares it with the code $F(D_s)$ stored in memory. If the above codes are equal, i.e. $R_e = F(D_s)$, then the transmission is considered to have been executed without errors. Otherwise the transfer is classified as erroneous.

The Boolean avalanche transformations in the proposed echoplex scheme are being used as a “single error amplifier” and their utilization ensures the increase of the Hamming distance between the correct and erroneous echo-codes. Correspondently, the probabilities of masking an error appearance during forward transmission by an error appearing during reverse transmission are decreased.

4 STATISTICAL SIMULATION FOR CHECKSUM AND ECHOPLEX ERROR DETECTION SCHEMES USING AVALANCHE TRANSFORMATIONS

Here the important aspect of the effectiveness of the proposed approach is to estimate the probability of error detection in checksum and echoplex schemes that use the avalanche transformations. Theoretical and experimental studies have been performed for obtaning such estimations.

According to the properties of avalanche transformation mentioned above, if one from its n bit inputs changes then about n/2 of its outputs will change also. However, there is a nonzero probability that a little more or less than n/2 of the output bits will change.

In the [7] was shown that the values of the probabilities that the dual and fourfold errors will not be detected using ordinary and modified checksum for 8 and 16 – bits length codes are shown in the Table I and Table II.

n	P_{2c}	P_{2f}	$t_2=P_{2c}/P_{2f}$
8	0.125	0.014286	8.75
16	0.0625	0.0000777	804.37

Table I

n	P_{4c}	P_{4f}	$t_4=P_{4c}/P_{4f}$
8	0.04296	0.001866	23
16	0.01123	$1.0122\cdot10^{-6}$	11094

Table II

In this paper a statistical simulation of the ordinary and proposed checksum schemes was performed. The results for the case, when the transferred block contains 256 bytes (n=8, k=256) and the appearance of single errors is subordinated to binomial model are shown in Table III and Fig. 3.

Table III

Probability of error appearance during one bit transmission -**p**	Statistical frequency of appearance of undetected errors	
	For ordinary checksum	For modified checksum
$2.0\cdot10^{-4}$	0.007009	0.000796
$3.0\cdot10^{-4}$	0.012964	0.001459
$4.0\cdot10^{-4}$	0.019007	0.002114
$5.0\cdot10^{-4}$	0.024571	0.002692
$6.0\cdot10^{-4}$	0.029363	0.003160
$7.0\cdot10^{-4}$	0.033263	0.003505
$8.0\cdot10^{-4}$	0.036256	0.003732
$9.0\cdot10^{-4}$	0.038389	0.003849
$10.0\cdot10^{-4}$	0.039741	0.003874
$11.0\cdot10^{-4}$	0.040406	0.003821
$12.0\cdot10^{-4}$	0.040481	0.003706
$13.0\cdot10^{-4}$	0.040062	0.003546
$14.0\cdot10^{-4}$	0.039236	0.003352
$15.0\cdot10^{-4}$	0.038084	0.003137

The graph in Fig. 3 shows the dependence of the statistical frequency of appearance of undetected errors from the probability of an error appearance during one bit transmission.

In the [6] was shown that the probability $(p\cdot(1-p)^{n-1})$ of a single error's appearance in a fixed bit position during the reverse transmission:

$$P_e^f = \frac{n^2\cdot p^2\cdot(1-p)^{2\cdot(n-1)}}{2^n} \quad (12)$$

The comparison between the obtained expression (12) and the formula (3) for the probability of an undetected single error's appearance by the traditional echoplex method shows that the utilization of the proposed approach makes it possible to increase the echoplex error detection reliability by q_0 times. The numerical value q_0 is determined by the following expression:

$$q_0 = \frac{P_e}{P_e^f} \approx \frac{2^n}{n} \quad (13)$$

So when the code length is n=8 the echoplex error detection reliability is increased by 32 times. When the code length is n=16 the probability of an undetected error is decreased by 4096 times.

The results of our statistical simulation of the proposed echoplex error detection scheme used in duplex channels are near to the previously presented theoretical results.

5 IMPLEMENTATION ANALYSIS

The implementation way of avalanche transformation significantly affects the efficiency of the proposed checksum and echoplex schemes. In order to implement in practice the proposed error detection scheme it is necessary to previously design Boolean avalanche transformations. This can be done

by using the known formalized methods of the Boolean SAC-functions synthesis [1], [2].

The Boolean avalanche transformations can be implemented using software or hardware. From the point of view of the data transmission rate, the hardware avalanche transformation using FPGA-implementation is the most effective. In contrast to CRC hardware implementation, the calculation of the Boolean SAC-functions can be executed in parallel.

The analysis has shown that the critical path for avalanche transformation's hardware implementation is equal to 4. Therefore the parallel hardware implementation of avalanche transformation ensures a time of execution that is significantly less in comparison to CRC.

In case of implementing the avalanche transformations using software when the length of transmitted codes is small (n=8), the calculation of the system of Boolean SAC-functions can be realized through tables. The truth tables of the SAC-functions may be stored in the transmitter's/receiver's EPROM or loaded to the transmitter's/receiver's RAM. If n=8 then the truth tables of the SAC-functions occupy a storage capacity of 256 bytes. In an avalanche transformation implemented by software, the execution time is some tens of nanosecons - less than the data transmission rate for the majority of digital channels.

The main advantages of the modified by proposed manner checksum in comparison to CRC is significant higher checking operation speed. Although the complexity of each Boolean function that satisfies the Strict Avalanche Criterion is higher than CRC, the structure of the operations allows widely parallel implementation. In so doing it is possible to realize a multilevel parallel implementation of checking operation as it is shown in Fig. 4.

This ensures to significantly increase the error checking operation speed compared to CRC.

6. BITSLICE TECHNOLOGY FOR BOOLEAN TRANSFORMATION IMPLEMENTATION

For calculating the systems of Boolean functions, which possess by avalanche effect, it is proposed to use the technology of bit parallelism. For this it is possible to synthesize Boolean SAC- functions in the form D -functions in accordance with the procedure [1]. The possibility of applying is caused by the fact that all functions of the chosen class have identical structure.

Let examine the calculation of the system of the orthogonal Boolean SAC-functions:

$$Y = ((A \times X) \bullet (\neg A \times X)) \oplus L \quad (14)$$

for $Y = \{y_1, y_2,\ldots, y_n\}$ – vector of the functions values;

$X = \{x_1, x_2,\ldots, x_n\}$ –vector of the input variables,
$A = \{a_{i,j}\}$, i,j=1…n –matrix of the coefficients;
$L = \{l_1, l_2,\ldots, l_n\}$ –vector of the linear parts;
«×» –matrix product;
«•» –element – by – element conjunction;
«¬» –inversion of the binary matrix

Let $\underline{Y}$, $\underline{V}_l$ and $\underline{V}_r$ – some of vector containing n of elements. Vector $\underline{L}$ – - contains the value of linear part on the tuples

$X = \{x_1, x_2,\ldots, x_n\}$

Let's define as A[i]- the i-th column of the matrix A.

The following algorithm is proposed for calculating the system (14):

ALGORITHM 1

START
STEP 0 $\underline{V_l} = 0$, $\underline{V_r} = 0$, $i = 1$
STEP 1 If $x_i = 0$, then go to STEP 3
STEP 2 $\underline{V_l} = \underline{V_l} \oplus A[i]$, $\underline{V_r} = \underline{V_r} \oplus not(A[i])$
STEP 3 $i = i + 1$
STEP 4 if $i \le n$, then go to STEP 1
STEP 5 $\underline{Y} = \underline{V_l} \bullet \underline{V_r} \oplus \underline{L}$
END

Calculation with the aid of the proposed algorithm of the system (14), which consists of eight functions, is illustrated by an example in Fig 5.

The characteristics of the computational complexity of algorithm can be improved, if one considers that, with the odd number of ones in vector $\underline{X}$, the vector $\underline{Z}$ = 0, and with even - $\underline{Z} = \underline{V}_l$. For calculating the system (14) it is possible to use the vector $\underline{V}_r$, after using the relationship:

$\underline{Y} = \underline{X}$ for $W(\underline{X})$ – odd
$\underline{Y} = \underline{X} \oplus \underline{V_l}$ for $W(\underline{X})$ – even

Thus, the calculation of $\underline{V}_l$ is necessary, only with even number of ones in vector $\underline{X}$.

For increase the effectiveness of the calculation of the systems (13), it is proposed to use the method of organizing the calculations with the preliminarily calculated tables. In this case the tables will be the sequence of operations of bit analysis, and the bit

analysis of vector X will be substituted by the word analysis, where word is address in the table.

Let's examine the table organization in more detail.

Let's introduce k of tables T_i of dimensionality m × n, moreover m•k=n. Let's fill them on the basis of matrix A according to the following formula.

$$T_i[Q]= \bigoplus_{\text{for } Qj=1} A[j] \quad i=1\ldots k,\ Q=0\ldots 2^m-1,\ j=m\bullet(i-1)+1,\ldots,m\bullet i$$

Let's introduce the following designations: Mask - vector, which contains ones into m low-order elements and zero in the rest; «→» - the operation of the shift of vector to the right (to the low-order bits).

The following algorithm of the calculation of the systems is proposed:

ALGORITHM 2

START

STEP 0 $Y = L,\ i = 1$

STEP 1 If $W(X)$ – odd, then END

STEP 2 $Q = (X \rightarrow ((i-1)\bullet m)) \bullet Mask$

STEP 3 $Y = Y \oplus T_i[Q]$

STEP 4 $i = i + 1$

STEP 5 If $i \leq k$, then go to STEP 2

END

The algorithm 2 has m of times larger productivity in comparison with algorithm 1. The work of algorithm 2 is illustrated by an example in Fig. 6. The proposed algorithms have linear computational complexity and that makes it possible to effectively realize avalanche transformations on any computational platform, including smart- carts.

7 CONCLUSION

The results of the presented studies which are directed toward an increase of the checksum and echoplex error detection reliability show that the utilization of avalanche transformations is an effective way of solving this problem.

The proposed approach does not demand the use of additional check bits. The increase in the reliability of error detection is achieved through the optimization of checkcode coding for channel in which the single arror appearance is diminated. The utilization of the avalanche transformation makes it possible to increase the Hamming distance between the correct checkcode and the checkcode which was destroyed by a single error. This allows a significant decrease in the probability of multi error masking interaction which is not detected by the ordinary checksum and echoplex methods.

The proposed approach allows the checksum and echoplex utilization to be more effective in comparison to CRC for high-speed data channels and control systems.

In principle, the suggested approach to increasing checksum and echoplex reliability can be utilized also when other types of errors are dominative.

References

[1] Bardis N.G, Mitrouli M, Maris Th.I., Orlova M.N., "Some properties of Boolean functions and design of cryptographically strong balanced Boolean functions", World Scientific and Engineering Society TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS, Issue 2, Volume 1, ISSN 1790-0832, pp: 717 – 723, August 2004

[2] Bardis N.G, Bardis E.G., Markovskaja N.A., Polymenopoulos A., "Design and Implementation of Boolean Balanced Functions Satisfying Strict Avalanche Criterion (SAC)", *Problem in Applied Mathematics and Computational Intelligence,* ISBN: 960-8052-30-0, pp. 12-16, 2001.

[3] Klove T., Korzhik V. Error Detecting Codes: General Theory and Their Application in Feedback Communication Systems. *Norwell, MA: Kluwer*,– pp.433, 1995.

[4] Saxena N.R., McCluskey E.J. "Extended precision checksums", *Proc.17-th Intern. Symp. Fault-Tolerant Computer*: FCTS-17,- Pittsburgrh(USA).- pp.142-147, 1987.

[5] Bardis N.G , "Echoplex Error Control System using Avalanche Transformations", TRANSACTIONS on COMMUNICATIONS, World Scientific and Engineering Society, Issue 2, Volume 3, ISSN 1109-2742, pp: 741 – 745, April 2004.

[6] Leros A., "Error Detection Control System based on CheckSum using Orthogonal Systems of SAC functions", World Scientific and Engineering Society TRANSACTIONS on COMMUNICATIONS, Issue 2, Volume 3, ISSN 1109-2742, pp: 789- 793, April 2004.

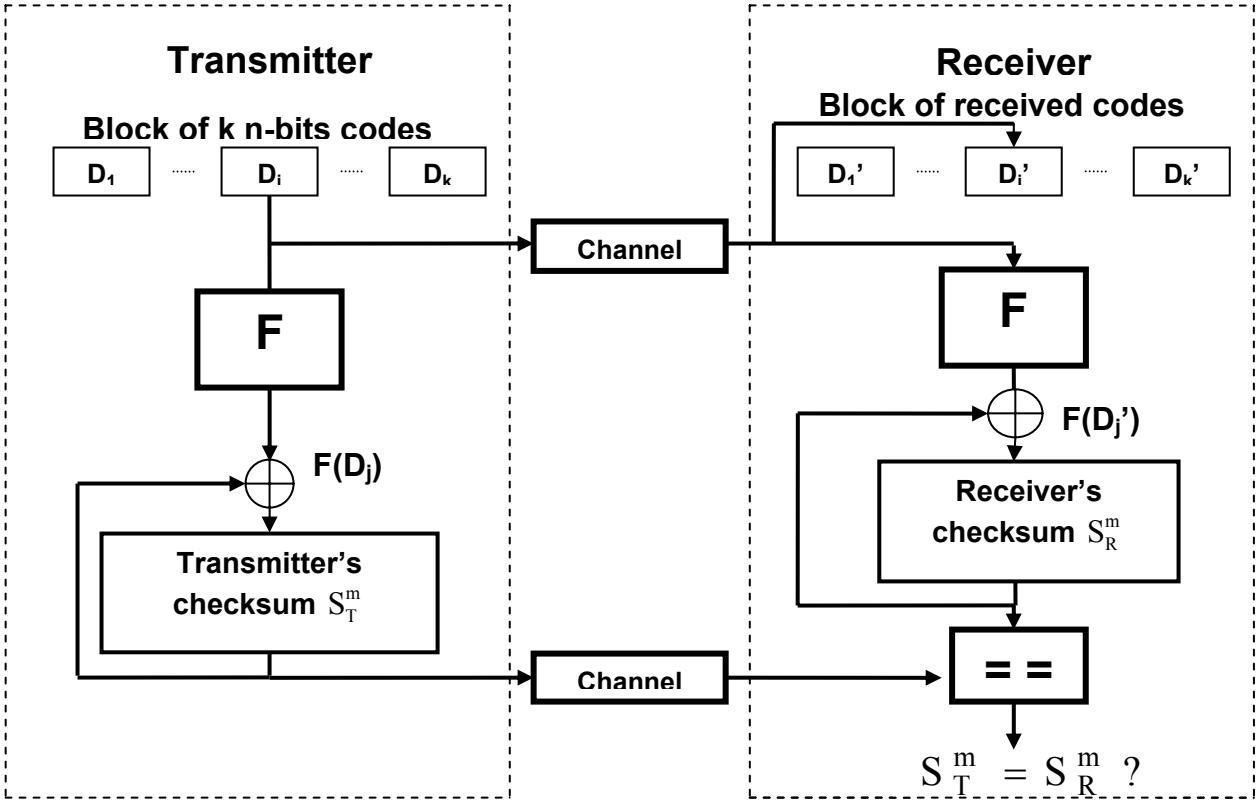

Transmitter
Block of k n-bits codes
D1 ..... Di ..... Dk
F
F(Dj)
Transmitter's checksum S_T^m
Channel
Channel
Receiver
Block of received codes
D1' ..... Di' ..... Dk'
F
F(Dj')
Receiver's checksum S_R^m
= =
$S_T^m = S_R^m$?

Fig. 1

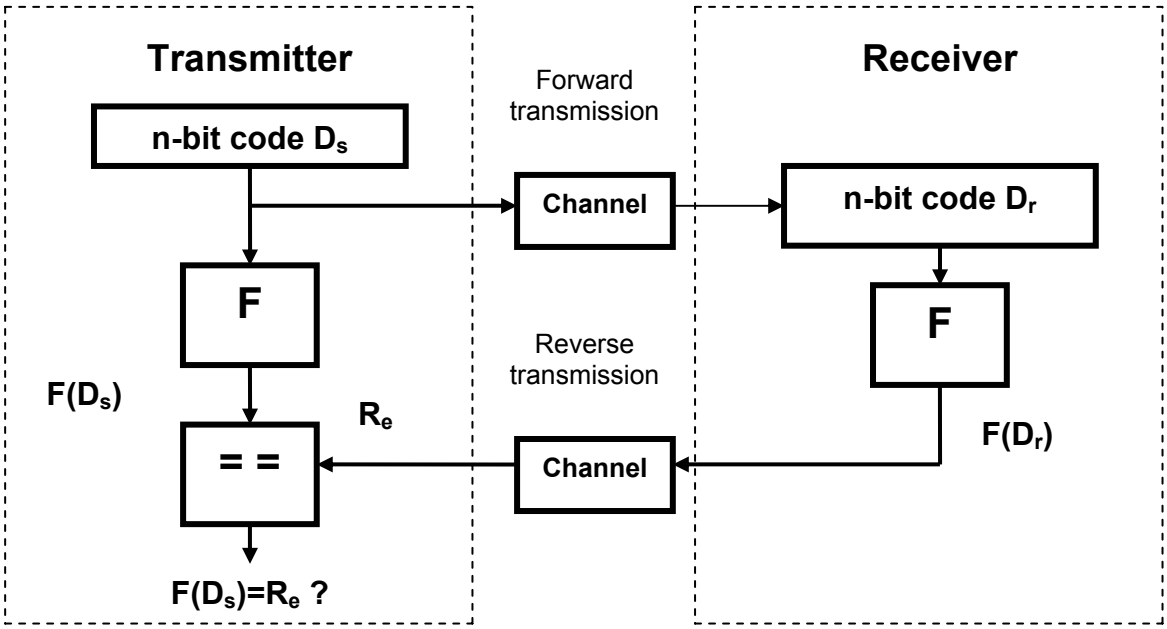

Transmitter
n-bit code Ds
F
F(Ds)
= =
Re
F(Ds)=Re ?
Forward transmission
Channel
Reverse transmission
Channel
Receiver
n-bit code Dr
F
F(Dr)

Fig. 2

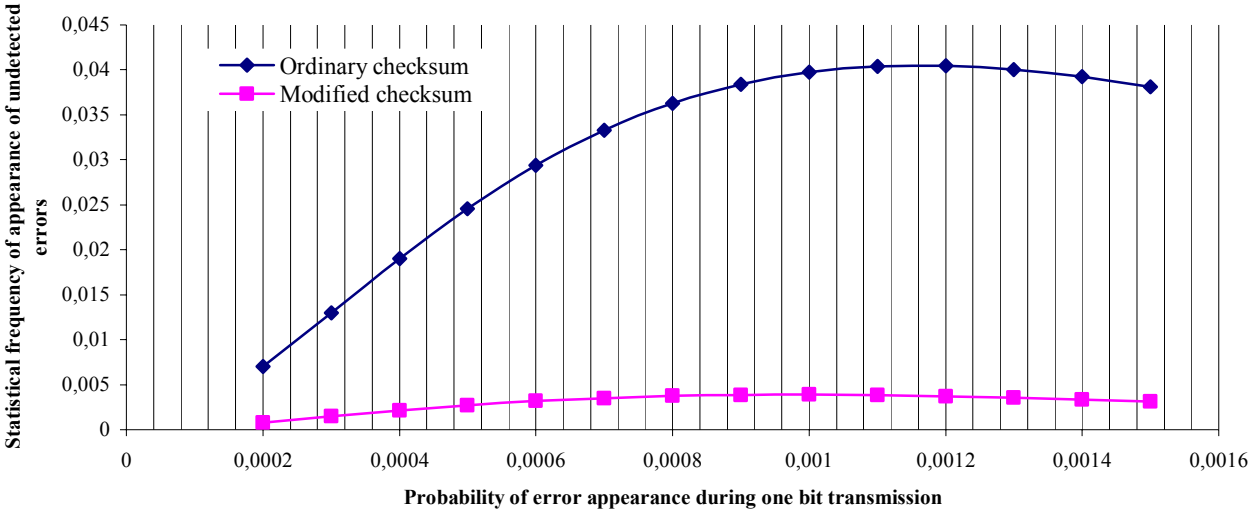
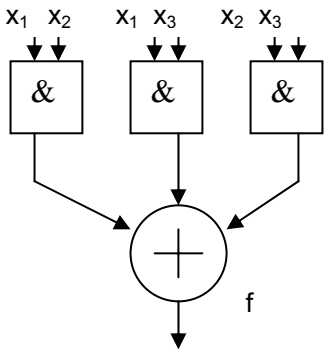


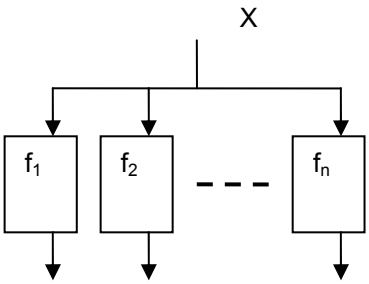
Fig. 3

Parallelization on the level of a single SAC-function computation

$f = x_1 \cdot x_2 \oplus x_1 \cdot x_3 \oplus x_2 \cdot x_3$



Parallelization on the level of a SAC-functions system computation



Parallelization on the level of the avalanche transformation of some serial transmitted codes

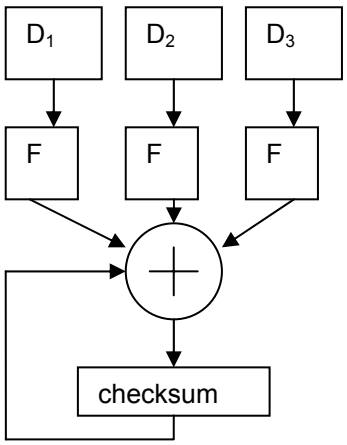


Fig 4

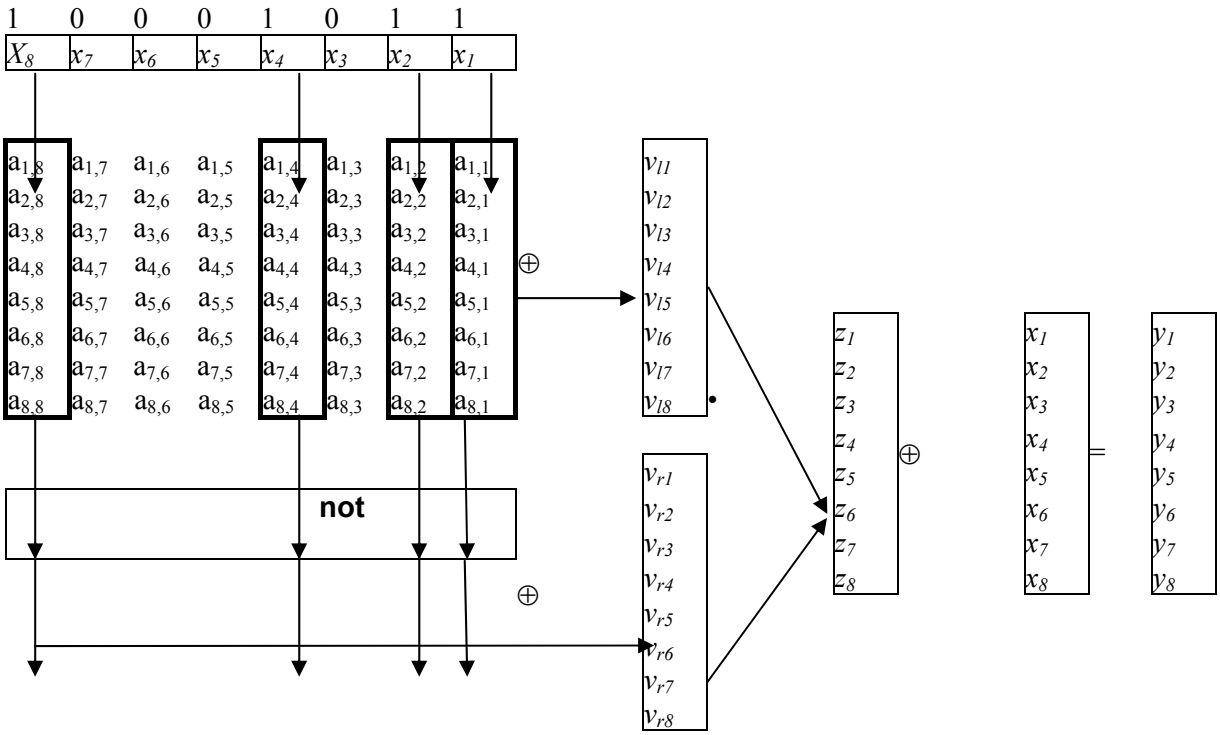


Fig. 5. Example of the calculation of the system of eight Boolean functions of the chosen class on the algorithm proposed

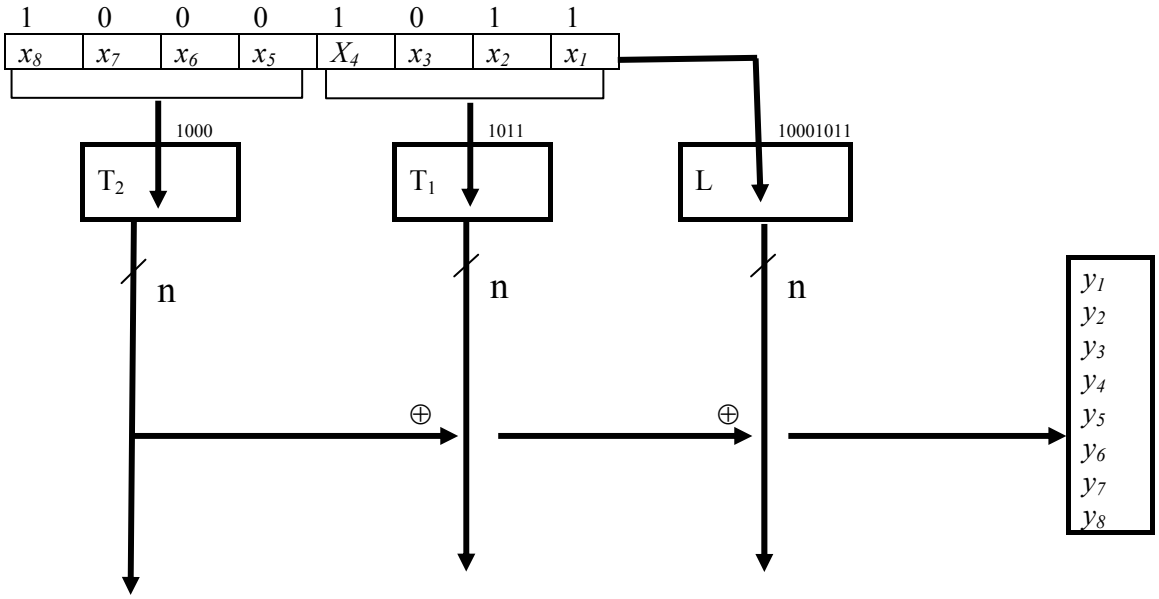


Fig. 6. Example of the calculation with the algorithm 2, the system of eight Boolean functions of the chosen class