Some properties of Boolean functions and design of Cryptographically strong balanced Boolean functions

Dr. N.G. BARDIS [1,2]
[1]Adjunct Assistant Professor
Department of Automation
Technological Educational Institution of Halkis
34400 Psahna, Halkis, Evia, Greece
[2]Research Associate
Hellenic Army Academy
Vari, 16673 Attiki, Greece

Dr. M.MITROULI
Assistant Professor
Department of Mathematics
National and Kapodistrian University of Athens
Panepistimiopolis, GR 15784 Athens, Greece

Dr. TH.I. MARIS
Assistant Professor
Department of Electrical Engineering
Technological Educational Institution of Halkis
34400 Psahna, Halkis, Evia, Greece

Dr. M.N. ORLOVA
Department of Applied Mathematics
National Technical University of Ukraine
37, Peremohy, pr. Kiev 03056, KPI
Ukraine

Abstract:- Properties of the total and conditional entropy – Strict Avalanche Criterion (SAC) are studied. The theorems that have been proved state the necessary and sufficient conditions for the total and conditional entropy (SAC) maximum of the special type functions, namely, D-functions. A procedure for synthesis of cryptographically strong balanced Boolean functions has been developed on the basis of the results obtained. It allows obtaining a more expanded class of Boolean functions for cryptographic application comparing to the known methods of synthesis

Key words: Boolean function, SAC function, balancedness, non-linearity.

1 Introduction

Most part of modern cryptographic algorithms, the block cipher, stream cipher and hash-algorithms among them, make use of Boolean transforms. Cryptoresistance to attacks by differential and linear cryptanalysis methods, depends on special properties of Boolean functions utilized in the algorithms.

The entropy characteristics and nonlinearity of Boolean functions determine these properties. A reasonable level of security with respect to the modern methods of attacks is provided by Boolean functions possessing high nonlinearity and the maximal entropy characteristics.

This work was supported by a grant by the Greek Ministry of Development - General Secretariat for Research and Technology and the European Community Social Funds. The main part of this work was carried out when the authors where attending the Operational program "Competitiveness" 2000 - 2006 ENTER 2001.

The latter property implies that a function attains the value of "zero" or "one" with equal probability and changes its value with alteration of the input parameters also with equal probability. Such functions have the zero level of auto-correlation and the only method for obtaining the reverse transform is total searching.

Obtaining Boolean functions with high nonlinearity and entropy characteristics is a difficult problem unsolved by the present time.

2 Problem statement

Of great practical importance is the development of some formalized methods for automatic generation of both single functions and systems of orthogonal functions of a large number (several hundreds) of variables applying arbitrary chosen keys.

Taking into account the large number of variables, the adequate methods for practical application should generate functions as algebraic normal forms (ANF) or in a procedure form, without utilizing the truth tables that require memory capacity exceeding the facility of modern computers.

The most significant criteria to evaluate the procedures from their practical application point of view are:

- ✓the qualitative characteristics of the generated functions (the value of the nonlinearity, the order of nonlinearity, the propagation properties);
- ✓the size of the computational recourses required;
- ✓the formalized character of the process of obtaining the required functions with regard to the key taken at random;
- ✓the maximal number of cryptographically strong functions that the method is able to generate;

By now a number of methods for synthesis of cryptographically strong Boolean functions have been suggested. Some of them, for example [2] provide for spectral Walsh-transforms application to obtain strong Boolean functions. Nevertheless such an approach cannot be adopted as a reasonable one from the technological aspect, since, in the course of synthesis of functions of n variables, with the tables of functions and spectra values whose capacity is in proportion to 2^n. The operation of reverse Walsh-transform, that is basic for this method, also requires time proportionally to 2^n.

Cryptographically strong Boolean functions may be obtained by means of bent-functions deconcatenation [1], however obtaining the bent-functions of a great number of variables as such is also a complex technological problem whose solution can be achieved only with expenditure of significant computational resources.

The heuristic methods of synthesis [4] are not suitable for automatic generation of functions in dependence on a randomly chosen key.

Nowadays, the most acceptable methods in practice for synthesis of ANF of cryptographically strong Boolean functions are the methods described in [3,5]. Their main shortcoming is that they enable only a small number of cryptographically strong functions from the total amount to be generated. The reason for that is that these methods are founded on the special properties of a restricted subset of cryptographically strong Boolean functions. To develop methods that allow for generating the most part of the cryptographically strong functions, a more thorough and overall investigation of their properties is necessary.

3 Basic Definitions and Properties of SAC-functions

The Hamming weight W $(f(x_1,\ldots,x_n)$ of a Boolean function $f(x_1,\ldots,x_n)$ of n variables is the total number of the values of "one" that the function attains on the 2^n possible tuples of the variables values that form the set Z

$$W(f(x_1,...,x_n)) = \sum_{x_1,...,x_n \in Z} f(x_1,...,x_n) \qquad (1)$$

The Boolean function $f(x_1,\ldots,x_n)$ satisfies the total entropy maximum criterion, i.e., is balanced if it takes the values of "zero" and "one" with equal probability:

$$W(f(x_1,...,x_n)) = 2^{n-1} \qquad (2)$$

The Boolean function $f(x_1,\ldots,x_n)$ satisfies the criterion of the conditional entropy maximum or Strict Avalanche Criterion (SAC), if alterating any of its n variables results in changing the value of the function with the probability of 0.5.

$$\forall x_j, j = 1,...,n : W(f(x_1,...,x_j,...,x_n) \oplus$$

$$\oplus f(x_1,...,\bar{x}_j,...,x_n)) = 2^{n-1} \qquad (3)$$

A system of Boolean functions $G=\{f_1(x_1,\ldots,x_n),f_2(x_1,\ldots,x_n),\ldots,f_n(x_1,\ldots,x_n)\}$ is an orthogonal one, if XOR of any subset of the system functions is a balanced function:

$$\forall \vartheta \subseteq G : W(\bigoplus_{f_j \in \vartheta} f_j(x_1,..., x_n)) = 2^{n-1} \qquad (4)$$

In this case the non-linearity, N $(f(x_1,\ldots,x_n))$, of the Boolean function $f(x_1,\ldots,x_n)$ is determined as the minimal Hamming's distance to the linear functions:

$$N(f(x_1,...,x_n)) = \min_{a_k \in \{0,1\}, k = 0,...,n} W(f(x_1,...,x_n) \oplus$$

$$\oplus (a_0 \oplus ... \bigoplus_{j = 1,...,n} a_j \cdot x_j)) \qquad (5)$$

4 D-functions

D-function of a power k is the sum of a linear function $L_0(X_0)$ and of the conjunction k of linear functions $L_1(X_1)$, $L_2(X_2),\ldots,L_k(X_k)$ that develop an orthogonal system:

$$f(X) = L_1(X_1) \cdot L_2(X_2) \cdot ... \cdot L_k(X_k) \oplus L_0(X_0) \qquad (6)$$

where $L_i(X_i)$ is a linear function determined on the set of variables $\{X_i\}$. The following special variants of D-functions exist:

D-function of the 1-st power is a linear function.

Degenerated D-function is a function, whose linear part $L_0(X_0)$ is a linear combination of the other components ($L_i(X_i)$, i=1…k):

$L_0(X_0)=a_0\oplus a_1\cdot L_1(X_1)\oplus a_2\cdot L_2(X_2)\oplus\ldots\oplus a_k\cdot L_k(X_k)$ (7)

Separated D-function is a function whose linear components of the conjunction ($L_i(X_i)$, i=0…k) are determined on non-overlapping tuples:

$$\{X_i\}\cap\{X_j\}=\varnothing,\ \forall\ i, j: i\neq j, i=1\ldots k, j=1\ldots k$$
$$\{X_1\}\cup\{X_2\}\cup\ldots\cup\{X_k\}=\{X\} \quad (8)$$

Lemma 1. Hamming's weight of a function-sum $F = f_1(x)\oplus f_2(x)$ is related to Hamming's weights of the functions-summands through the following relation:

$$W(f_1(x)\oplus f_2(x))=W(f_1(x))+W(f_2(x))-2W(f_1(x)\cdot f_2(x)) \quad (9)$$

Corollary 1.(Generalization of Lemma 1 for 3 functions):

$$W(f_1(x)\oplus f_2(x)\oplus f_3(x))=$$
$$= W(f_1(x)) + W(f_2(x)) + W(f_3(x)) -$$
$$- 2\,[W(f_1(x)\cdot f_2(x))+W(f_2(x)\cdot f_3(x))+ +W(f_3(x)\cdot f_1(x))]+ 4W(f_1(x)\cdot f_2(x)\cdot f_3(x)) \quad (10)$$

Corollary 2.(Generalization of Lemma 1 for m functions):

$$W(\bigoplus_{j=1}^{m} f_j(x)) = \sum_{j=1}^{m}(-1)^{j-1}\cdot 2^{j-1}\cdot \cdot \sum_{j1\neq j2\neq\ldots\neq ji} W(f_{i1}(x)\cdot f_{j2}(x)\cdot\ldots\cdot f_{ij}(x)) \quad (11)$$

Lemma 2. Hamming's weight of the conjunction of k variables $F = x_1\cdot x_2\cdot\ \ldots\ \cdot x_k$ is equal to:

$$W(F) = 2^n/2^k = 2^{n-k} \quad (12)$$

Corollary 3. Hamming's weight of the function-product $F = f_1(x)\cdot\ f_2(x)\cdot\ \ldots\ \cdot f_k(x)$ is equal to 2^{n-k} if functions $f_i(x)$, I=1,…,k develop an orthogonal system.

Theorem 1. The necessary and sufficient condition for a D-function to satisfy the total entropy maximum, that is to be a balanced one, is its property of non-degeneracy, that is the linear component $L_0(X_0)$ of the D-function and the linear functions $L_1(X_1)$, $L_2(X_2)$,…,$L_k(X_k)$ must compose an orthogonal system.

Proof.

Present the D-function as a XOR of 3 component:

$$F(X) = F_1(X)\oplus F_2(X)\oplus F_3(X) \quad (13)$$

, where

$F_1(X) = L_1(X_1)\cdot L_2(X_2)\cdot\ \ldots\ \cdot L_k(X_k)$

$F_2(X)=c_0\oplus c_1\cdot L(X_1)\oplus c_2\cdot L_2(X_2)\oplus\ldots\oplus c_k\cdot L_k(X_k)$, is a part of a linear function representable in form of the linear combination of the conjunctive part components $L_0(X_0)$, $c_h\in\{0,1\}$,h=0,…k ,

$F_3(X)=L_0(X_0)\oplus F_2(X)$ - is a part of linear function $L_0(X_0)$ non-representable in form of linear combination of the multiplicative part components.

Necessity.

Make use of the proof method from the opposite. Suppose, function (13) is a degenerated D-function. In a degenerated function the component $F_3(X) = 0$. Apply Lemma 1 for determining the number of ones in the function: $W(F(X)) = W(F_1) + W(F_2) - 2W(F_1F_2)$.

According to Corollary 3: $W(F_1) = 2^{n-k}$. Since $F_2(X)$ is a linear function, then Hamming's weight F_2 equals $W(F_2) = 2^{n-1}$. Representation of functions $F_1(X)$ и $F_2(X)$ is a logical product of the conjunctive components $L_1(X_1)$,…,$L_k(X_k)$ by a linear function of $L_1(X_1)$,…,$L_k(X_k)$:

$$F_1(X)\cdot F_2(X) = \prod_{j=1}^{k} L_j(X_j)\cdot(c_0\oplus \bigoplus_{j-1}^{k} c_j\cdot L_j(X_j)) \quad (14)$$

If the number of the non-zero components is even, then $F_2(X)=0$, and, correspondingly, $F_1(X)\cdot F_2(X)=0$, otherwise $F_1(X)\cdot F_2(X)=F_1(X)$ and accordingly to (12)

$W(F_1(X)\cdot F_2(X))=W(F_1(X))=2^{n-k}$.

In the first case $W(F(X)) = 2^{n-k} + 2^{n-1} + 2\cdot 0 =2^{n-1} +2^{n-k}$, and correspondingly, in the other one $W(F(X))=2^{n-k}+ 2^{n-1}-2\cdot 2^{n-k}=2^{n-1}-2^{n-k}$.

Thus, in both cases function (13) appears to be non-balanced. Consequently, the assumption about the degeneracy of the initial function is false. Therefore, to satisfy the unconditional entropy maximum criterion, the D-function must be non-degenerated, which proves the theorem.

Sufficiency.

Since function $L_0(X_0)$ does not depend linearly on the conjunctive components $L_1(X_1)$,…,$L_k(X_k)$, they altogether develop a system of k+1 orthogonal functions, so transition to a new coordinates system $\{Z\}^{k+1}$ is quite rightful, here

$$z_j = L_j(X_j), j = 1,...,k$$

$$z_{k+1} = L_0(X_0) \tag{15}$$

In the new coordinates system, the D-function has the form: $F(Z) = z_1 \cdot z_2 \cdot \ldots \cdot z_k \oplus z_{k+1}$, that is, it represents the XOR of the balanced function (z_{k+1}) and the function ($z_1 \cdot z_2 \cdot \ldots \cdot z_k$) that does not depend on the former one and, therefore, the D-function is a balanced one. Since the number of "ones" in the function does not depend on the form of its representation, the non-degenerated D-function under consideration meets the unconditional entropy maximum criterion, which proves the statement. $N(f) = 2^8 - 2^4 = 240$.

5 D-functions of the 2-nd power

Consider a special case of D-functions, namely, functions of the second power.

$$f(X) = L_1(X_1) \cdot L_2(X_2) \oplus L_0(X_0) \tag{16}$$

Theorem 2. D-function of the 2nd power satisfies the criterion of conditional entropy maximum, that implies it is always a SAC-function if $X_1 \cup X_2 = \{x_1, \ldots, x_n\}$.

Proof. For the proof, let us make use of a known statement [5] that if for all x_j, $j=1,2,\ldots,n$, at representation of function $f(X)$ in the form: $f(X) = g_j(X) + x_j \cdot h_j(X)$, (here $g_j(X)$, $h_j(X)$, are functions that do not depend on x_j), functions $h_j(X), j=1,\ldots,n$ are balanced ones, then $f(X)$ meets the conditional entropy maximum criterion, so it is a balanced SAC-function. Let $x_j \in X_1$, $x_j \notin X_2$, then function $L_1(X_1)$ may be represented in the form $L_1(X_1)=x_j \oplus R_j(X_1\text{-}x_j)$, correspondingly $f(X)=(x_i \oplus R_1(X_1\text{-}x_j)) \cdot L_2(X_2) \oplus L_0(X_0)=x_j \cdot L_2(X_2) \oplus g_j(X)$. Since the function $L_2(X_2)$ is linear and correspondingly balanced, independent of x_j, so with respect to the variable x_j function $f(X)$ corresponds to SAC. It may be proved in the similar way that function $f(X)$ is a SAC-function, if variable $x_j \in X_2$, $x_j \notin X_1$.

If $x_j \in X_2$, $x_j \in X_1$, then

$f(X)=(x_j \oplus R_1(X_1\text{-}x_j)) \cdot (x_j \oplus R_2(X_2\text{-}x_j)) \oplus L_0(X_0)=$
$=(x_j \oplus R_1(X_1\text{-}x_j)) \cdot (x_j \oplus R_2(X_2\text{-}x_j)) \oplus L_0(X_0) \oplus R_1(X_1\text{-}x_j) \cdot R_2(X_2\text{-}x_j) \oplus x_j \cdot (1 \oplus R_1(X_1\text{-}x_j) \oplus R_2(X_2\text{-}x_j))=$
$=x_j \cdot (1 \oplus R_1(X_1\text{-}x_j) \oplus R_2(X_2\text{-}x_j)) \oplus g_j(X)$, that is the multiplier at x_j in this case as well appears to be a linear function, and correspondingly, a balanced one, because $R_1(X_1\text{-}x_j) \neq R_2(X_2\text{-}x_j)$, in view of $L_1(X_1) \neq L_2(X_2) \Rightarrow (x_j \oplus R_1(X_1\text{-}x_j)) \neq (x_j \oplus R_2(X_2\text{-}x_j))$.

So, D-function of the second power (16), for which the condition $X_1 \cup X_2 = \{x_1, \ldots, x_n\}$ is held, is always a SAC–function .

For example, consider synthesis of a function of 4 variables. Let $L_1=x_1 \oplus x_2 \oplus x_3$, $L_2=x_1 \oplus x_4$, $L_0(X)=x_2$. Then $f(x)=(x_1 \oplus x_2 \oplus x_3) \oplus (x_1 \oplus x_4) \oplus x_2 = x_1 \oplus x_2 \oplus x_1 \cdot x_4 \oplus x_1 \cdot x_2 \oplus x_2 \cdot x_4 \oplus x_1 \cdot x_3 \oplus x_3 \cdot x_4$.

6 Compound D-functions

Consider a Boolean function that is a XOR of a linear function $L_0(X_0)$, of the product of liner functions $L_1(X_1)$ and $L_2(X_2)$ such that $X_1 \cup X_2 = \{x_1, \ldots, x_n\}$ and of the product k ($k \leq n-3$) of linear functions $L_3(X_3), L_4(X_4), \ldots, L_{k+2}(X_{k+2})$, in this case all the functions L_j, $j=0,\ldots,k+2$ develop a system of linearly-independent functions.

$$f(X) = L_0(X_0) \oplus L_1(X_1) \cdot L_2(X_2) \oplus \prod_{i=3}^{k+2} L_i(X_i) \tag{17}$$

Demonstrate that such a Boolean function satisfies the conditional and unconditional entropy maximum criterion.

Since all the linear functions $L_0(X_0), \ldots, L_{k+3}(X_k)$ are linearly-independent, transition to a new coordinate system $\{Z\}$: $z_j=L_j(X_j), j=0,\ldots,k+2$ is lawful.

$$f(Z) = z_0 \oplus z_1 \cdot z_2 \oplus z_3 \cdot z_4 \cdot \ldots \cdot z_{k+2} \tag{18}$$

Since function (18) is a XOR of a balanced function (z_0) and a function independent of the variables of the balanced function, then function (18) is a balanced one. Since the number of "ones" does not depend on the representation of the function, the function (17) satisfies the criterion of unconditional entropy maximum.

Now disclose that function (18) satisfies the criterion of conditional entropy maximum. For this, just as at proof of Theorem 2, it is necessary to reveal that for all x_j, $j=1,2,\ldots,n$, at representing the function $f(X)$ in the form: $f(X)=g_j(X)+x_j \cdot h_j(X)$, the function $h_j(X)$ is a balanced one.

If $x_j \notin \{X_3, X_4, \ldots, X_{k+2}\}$, then the course of the proof is quite identical to that of Theorem 2 presented above. If $x_j \in \{X_3, X_4, \ldots, X_{k+2}\}$, then on introducing the following symbols for the linear functions $R_i(X_i)=L_i(X_i)$, $\delta_i=0$ if $x_j \notin X_i$ and $R_i(X_i\text{-}x_j)=L_i(X_i) \oplus x_j$, $\delta_i=1$ if $x_j \in X_i$ for $i=1,\ldots,k+2$, the function $h_j(X)$ independent of x_j may be represented as

$$h_j(X) = \delta_1 \cdot R_2(X) \oplus \delta_2 \cdot R_1(X)$$

(19)

$$\oplus \sum_{t=3}^{k+2} \delta_t \cdot \prod_{\substack{l=3 \\ l \neq t}}^{k+2} R_l(X)$$

Since all the functions R_l, l=1,…,k+3 composing (19) are linearly-independent, then, according to Theorem 1, each of the functions h_j, j=1,…,n is balanced, and consequently the function determined by (17) possesses the conditional entropy maximum, so it is a SAC-function.

The theoretical results obtained make it possible to formulate the following procedure for obtaining Boolean functions possessing the maximum of the total and conditional entropy:

On the set of $\{x_1,\ldots,x_n\}$ variables, $3 \le t \le n$ linear Boolean functions are built that develop an orthogonal system , and in doing so the union of variables set comprised in the linear function $L_1(X_1)$ and $L_2(X_2)$ must compose the total set of the variables $X_1 \cup X_2=\{x_1,x_2,\ldots,x_n\}$.

Accordingly to (18), the normal algebraic form is built of the Boolean function that corresponds to the criterion of the total and conditional entropy maximum, or, in other words, is a balanced SAC-function.

The procedure suggested for balanced Boolean SAC-functions is illustrated by the following example of synthesis of a balanced function of six variables (n=6). According to item 1, a system of k=n=6 linear Boolean functions is built that develop an orthogonal system: $L_0(x_1)=x_1$, $L_1(x_1,x_2,x_3)=x_1\oplus x_2\oplus x_3$, $L_2(x_4,x_5,x_6) = x_4\oplus x_5\oplus x_6$, $L_3(x_3,x_4)=x_3\oplus x_4$, $L_4(x_2)=x_2$, $L_5(x_4,x_6)=x_4 \oplus x_6$. In correspondence with (18) the balanced SAC–function is built in the form: $f(X)=x_1\oplus (x_1\oplus x_2\oplus x_3)\cdot(x_4\oplus x_5 \oplus x_6) \oplus x_2\cdot(x_4\oplus x_3)\cdot(x_4\oplus x_6)=x_1\oplus x_1\cdot x_4\oplus x_1\cdot x_5\oplus x_1\cdot x_6\oplus x_2\cdot x_5\oplus x_2\cdot x_6\oplus x_3\cdot x_4\oplus x_3\cdot x_5\oplus x_3\cdot x_6\oplus x_2\cdot x_4\cdot x_6\oplus x_2\cdot x_3\cdot x_4\oplus x_2\cdot x_3\cdot x_6$. The non-linearity of the function synthesized is 20, and the non-linearity order is equal to 3.

7 Superposition of the functions

The suggested approach may be generalized for synthesis of functions in the orthogonal spaces of other functions.

Let there exist:

a) an orthogonal system of n functions $\{Z\}^n$

b) an arbitrary function of (n-1) variables $S^{n-1}(X)$

Then the next superposition will be balanced:

$$F(X) = S(z_1, z_2, \ldots, z_{i-1}, z_{i+1}, \ldots, z_n) \oplus z_i \qquad (20)$$

Theorem 3. Let there exist the following k ($3 \le k \le n$) functions of n variables $X^n=(x_1\ldots x_n)$:

$Z_1(X^n)=\Phi_1^j(x_1\ldots x_{j-1}x_{j+1}\ldots x_n)\oplus$
$\oplus x_j\cdot\Psi_1^j(x_1\ldots x_{j-1}x_{j+1}\ldots x_n)$, with j=1…n;

$Z_2(X^n)=\Phi_2^j(x_1\ldots x_{j-1}x_{j+1}\ldots x_n)\oplus$
$\oplus x_j\cdot\Psi_2^j(x_1\ldots x_{j-1}x_{j+1}\ldots x_n)$,with j=1…n;

$Z_3(X^n)=\Phi_3^j(x_1\ldots x_{j-1}x_{j+1}\ldots x_n)\oplus$
$\oplus x_j\cdot\Psi_3^j(x_1\ldots x_{j-1}x_{j+1}\ldots x_n)$,with j=1…n;

$Z_k(X^n)=\Phi_k^j(x_1\ldots x_{j-1}x_{j+1}\ldots x_n)\oplus$
$\oplus x_j\cdot\Psi_k^j(x_1\ldots x_{j-1}x_{j+1}\ldots x_n)$, with j=1…n;

(21)

,denominate

$\xi(X^{n-1})=\Phi_2^j(X^{n-1})\cdot\Psi_3^j(X^{n-1})\oplus\Phi_3^j(X^{n-1})\cdot\Psi_2^j(X^{n-1})\oplus$
$\oplus\Psi_2^j(X^{n-1})\cdot\Psi_3^j(X^{n-1})\oplus\Psi_1^j(X^{n-1})$

In this case:

function $Z_1(X^n)$ is balanced;

functions $\{Z\}$ are mutually independent;

in the set of functions $\Phi_i^j(X^{n-1})$ and $\Psi_i^j(X^{n-1})$, i=4…k $\forall$ j=1…n , there exists a certain subset $\{W_j\}$ (of m_j functions) all the functions of which are mutually independent. Moreover, the functions that do not enter the subset $\{W_j\}$ may be represented through a sum of function from set $\{W_j\}$.

Function $\xi(X^{n-1})$ is balanced and independent of the set of functions $\{W_j\}$, $\forall$ j=1…n;

Then the following function satisfies the conditional and total entropy maximum criterion:

$$F(X^n) = S(y_1, \ldots, y_{k-3}) \oplus Z_3(X^n) \cdot Z_2(X^n) \oplus Z_1(X^n) \qquad (22)$$

,where

S – an arbitrary function of(k-3) variables

$y_i = Z_{i+3}(X^n)$, i=1…k-3

Proof.

Since functions (21) are mutually independent, transition is possible to a new coordinate system $X^n \to Z^k$ where function (22) is equivalent to the following one:

$$F(X^n) \equiv F(X^k) = S(Z_4, \ldots, Z_k) \oplus Z_2 \cdot Z_3 \oplus Z_1 \qquad (23)$$

This function is balanced because it consists of the sum of the balanced function (Z_1) and a function independent of the variables of the balanced function Z_1. Since the balancedness of a function does not depend on its representation, function (23) satisfies the total entropy maximum criterion, which proves the theorem.

Present function (20) in the form: $F(X^n) = U_S^j(X^{n-1}) \oplus U_{Z3\bullet Z2}^j(X^{n-1}) \oplus U_{Z1}^j(X^{n-1}) \oplus x_j\cdot[V_S^j(X^{n-1}) \oplus V_{Z3\cdot Z2}^j(X^{n-1}) \oplus V_{Z1}^j(X^{n-1})]$. Consequently, function (20) satisfies the conditional entropy maximum criterion if the following function satisfies the total entropy maximum criterion for any j:

$$P(X^{n-1}) = V_S^j(S^{n-1}) \oplus V_{Z2\cdot Z3}^j(X^{n-1}) \oplus V_{Z1}^j(X^{n-1}) \quad (24)$$

The following identity is lawful: $V_{Z3\cdot Z2}^j(X^{n-1}) \oplus V_{Z1}^j(X^{n-1}) \equiv \xi$. The function $V_S^j(X^{n-1})$ appears to be a certain superposition of the functions $\Phi_i^j(X^{n-1})$ and $\Psi_i^j(X^{n-1})$, i=4…k. According to the theorem conditions, there exists a subset of functions $W_j=\{w_1\ldots w_{mj}\}$ that are mutually independent, while the other functions are representable by their combination. Consequently, the identity: $V_S^j(X^{n-1}) \equiv V_S^j(W^{mj})$ is rightful. Thus, function (24) is equivalent to the sum of two functions: $P(X^{n-1}) \equiv V_S^j(W^{mj}) \oplus \xi$. Furthermore, according to the theorem conditions, function ξ is independent of the functions of set W, and the functions of set W, in their turn, are mutually independent. Consequently, if denote $\xi=w_{mj+1}$, then the transition to a new coordinates system: $X^n \rightarrow W^{mj+1}$ is possible. In this coordinates system function (24) is a sum of the balanced function ($\xi=w_{mj+1}$) and a function that does not depend on the variable w_{mj+1}. This fact ensures the balancedness of function (24) at any j and implies, in its turn, that function (20) satisfies the conditional entropy maximum criterion.

The nonlinearity of the functions like (20) may be shown to be equal 2^{n-2}.

8 Conclusions

The formalized method suggested for obtaining SAC-functions of high nonlinearity is based on utilizing the generation of function properties with the maximum of the total and conditional entropy for the orthogonal Boolean spaces. The method operates with ANF, which on the one hand removes the technological restrictions on obtaining functions of a large number of variables (the experiments carried out have proved the practical possibility to obtain cryptographically strong functions of hundreds variables with use of personal computers) and on the other hand makes it possible to obtain functions most suitable for computation.

Comparing to the known methods for obtaining cryptographically strong functions, the suggested one requires much less computational resources. So, comparing to one of the most effective methods of synthesis [3], the suggested one provides the performance by about two orders higher.

The significant advantage of the presented approach comparing to the known ones [2,3,5] is that it allows the generation of an appreciably larger number of balanced SAC-functions from all the possible at a given number of n variables. So, for n=4, the method suggested may synthesize above 200 functions, while the method described in [5] provides developing only 96 functions, and method [3] does only 72 ones.

References

1. Cusic T.W. On construction of balanced correlation immune function, in sequences and their application. // Proceeding of SETA'98-Springer Discrete Mathematics and Theoretical Computer Sciences,-1999-P.184-190.
2. Forre R. The strict avalanche criterion: spectral properties of Boolean functions and extended definition // Advances in Cryptology – Crypto'88 Proceeding, Lecture Notes in Computer Sciences, 403 – 1990 P.450-468.
3. Kurosawa K., Satoh T. Design of SAC/PC(l) of Order k Boolean Functions and Three Other Cryptographic Criteria.// Advances in Cryptology –Eurocrypto'97 Proceeding, Lecture Notes in Computer Science 1233-1997-P.433-449.
4. Millan W., Clark A., Dawson E. Heuristic design of cryptographically strong balanced Boolean functions // Advanced of Cryptology – Eurocrypt'98 Proceeding Lecture Notes in Computer Sciences, 1403 – 1998 P. 485-499.
5. Polymenopolos A., Bardis N.G, Bardis E.G., Markovskaja N.A. Design and Implementation of Boolean Balanced Function Satisfying Strict Avalanche Criterion (SAC) – Problems in Applied Mathematics and Computational Intelligence. WSESP, 2000, P.12-16.