A Class of Data-Dependent Operations

Nikolay A. Moldovyan, Alexander A. Moldovyan, and Michael A. Eremeev
(Corresponding author: Nikolay A. Moldovyan)

Specialized Center of Program Systems "SPECTR"
Kantemirovskaya, 10, St.Petersburg 197342, Russia (Email: nmold@cobra.ru)

(Received July 19, 2005; revised and accepted Aug. 25, 2005)

Abstract

This paper introduces a new class of the controlled primitives that are oriented to the use in the form of the data-dependent operations while designing fast hardware-suitable ciphers. The proposed class represents a generalization of the known data-dependent permutations. New primitives are used to design switchable controlled operations and ciphers with simple key scheduling.

Keywords: controlled primitives, data-dependent operations, switchable operations, simple key scheduling, fast block ciphers

1 Introduction

Well known permutation networks (PNs) have been widely studied in the field of parallel processing and telephone switching systems [4, 12, 19] and they are very interesting to be used as controlled cryptographic primitive. The PNs are well suited for cryptographic applications, since they allow one to specify and perform permutations at the same time. A variant of the symmetric cryptosystem based on PNs controlled with key is presented in [13]. Another cryptographic application of PN is presented by the cipher ICE [9] in which a very simple PN is used to specify a key-dependent permutation, the last is not very effective against differential cryptanalysis [16] though. More advanced cryptographic application of the PNs is using them in the form of the data-dependent permutations (DDPs) [11]. Efficiency of the use of data-dependent operations (DDOs) was demonstrated with examples of ciphers RC5 [14], RC6 [15], and MARS [3], which are based on data-dependent rotations with 32 different modifications. The PNs can be used as controlled permutation (CP) boxes to perform DDP. It is easy to design the CP boxes providing possibility to specify $2^{64}...2^{192}$ and more different modifications of the DDP operation on data bit strings [11] and key bit strings [10]. Recently published detailed results on investigating DDPs and on their application show that DDPs are well suited to design fast ciphers oriented to cheap hardware implementation [5, 8, 17]. However all mentioned above primitives conserves the weight of the transformed bit strings. Thus, it is very interesting to develop and study DDP-like DDOs that change arbitrary the weight of the transformed binary vectors.

This paper introduces a new class of the DDP-like controlled primitives defining transformations with the substitution properties.

In Section 2 we consider a layered topology of the operational boxes implementing the DDP-like primitives possessing the substitution properties. The new primitives are called controlled operational substitutions (COSes), since they are free of preserving the weight of the input binary vector. The COS boxes are constructed using some layered CP box as a prototype and replacing all switching elements by elementary controlled 2×2 **S**-boxes denoted as $\mathbf{F}_{2;1}$. Selecting different types of the main building blocks $\mathbf{F}_{2;1}$ one can design different DDP-like primitives. Several criteria are formulated to select $\mathbf{F}_{2;1}$-boxes. The criteria are used to classify all possible variants of the $\mathbf{F}_{2;1}$-boxes. Non-linear and differential properties of different types of the $\mathbf{F}_{2;1}$-boxes are presented.

In Section 3 we consider design and properties of the COS boxes having the first-order topology.

Section 4 discusses design of the switchable COS-box operations and presents several COS-based block ciphers.

Section 5 presents conclusion that proposed new class of the DDOs gives more design possibilities than DDPs while developing fast cheap-hardware-oriented ciphers. The COSes suit well to design of the switchable DDOs the use of which allows preventing weak keys in the ciphers with simple key scheduling.

Notation: Let BF^n or f^n denote Boolean function (BF) in n variables, i.e. $f^n = f(x_1, x_2, ..., x_n)$.

Let the binary vector $(f(0,0,0), f(0,0,1), f(0,1,0), f(0,1,1), f(1,0,0), f(1,0,1), f(1,1,0), f(1,1,1))$ denote truth table of the BF $f(x_1, x_2, x_3)$.

Let NL(f^n) denote non-linearity of f^n in the sense of the minimal distance from f^n to the set of the affine BFs^n. The distance between two BFs f_1^n and f_2^n is the weight of the truth table of the BF $f_3^n = f_1^n \oplus f_2^n$.

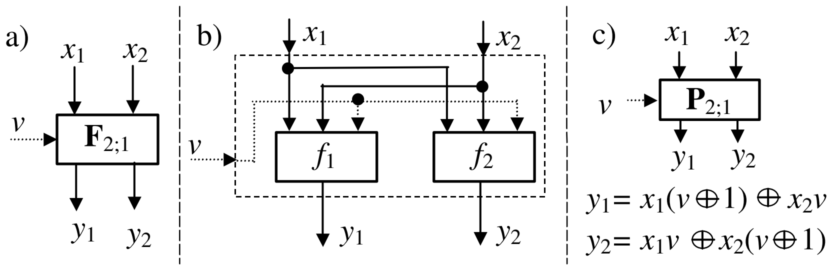

Figure 1: Elementary box $\mathbf{F}_{2;1}$: a − designation, b − representation as a pair of BFs^3, c − switching element $\mathbf{P}_{2;1}$

Let hexidecimal numbers denote truth tables of BF^n. For example 35 and CA denotes truth tables (00110101) and (11001010), respectively.

Let $\{0,1\}^n$ denote the set of all n-bit binary vectors $X = (x_1, ..., x_n)$.

Let numerical value (or simply value) X be $\sum_{i=1}^{n} x_i 2^{i-1}$.

Let $\lfloor \rho \rfloor$ denote the maximum even integer less or equal to ρ.

Let $X \oplus Y$ denote the bit-wise XOR operation performed on X and Y : $X, Y \in \{0,1\}^n$.

Let $(A, B, ..., Z)$ denote concatenation of the binary vectors A, B,..., Z.

Let "$+_n$" ("$-_n$") denote addition (subtraction) modulo 2^n.

Let $Y = X^{>>>k}$ denote rotation of the word X by k bits, where $\forall i \in \{1, ..., n-k\}$ we have $y_i = x_{i+k}$ and $\forall i \in \{n-k+1, ..., n\}$ we have $y_i = x_{i+k-n}$.

Definition 1. *Let $\{\mathbf{F}_1, \mathbf{F}_2, ..., \mathbf{F}_{2^m}\}$ be some set of the single-type operations defined by formula $Y = \mathbf{F}_i = \mathbf{F}_i(X_1, X_2, ..., X_q)$, where $i = 0, 1, ..., 2^m - 1$ and $X_1, X_2, ..., X_q$ are the input n-dimensional binary vectors (operands) and Y is the output n-dimensional binary vector. Then the V-dependent operation $\mathbf{F}^{(V)}$ defined by formula $Y = \mathbf{F}^{(V)}(X_1, X_2, ..., X_q) = \mathbf{F}_V(X_1, X_2, ..., X_q)$, where V is the m-dimensional controlling vector, we call the controlled q-place operation. The operations $\mathbf{F}_0, \mathbf{F}_1, ..., \mathbf{F}_{2^m-1}$ are called modifications of the controlled operation $\mathbf{F}^{(V)}$.*

Definition 2. *Let $\{\mathbf{F}_0, \mathbf{F}_1, ..., \mathbf{F}_{2^m-1}\}$ be the set of the modifications of the controlled operation $\mathbf{F}^{(V)}$. The operation $(\mathbf{F}^{-1})^{(V)}$ containing modifications $\mathbf{F}_0^{-1}, \mathbf{F}_1^{-1}, ..., \mathbf{F}_{2^m-1}^{-1}$ is called inverse of $\mathbf{F}^{(V)}$, if for all V $\mathbf{F}_V^{-1}$ and $\mathbf{F}_V$ are mutual inverses.*

Definition 3.[10] *Let given the CP-box operation $Y = \mathbf{P}_{n;m}^{(V)}(X)$, where $X, Y \in \{0,1\}^n$. The CP box $\mathbf{P}_{n;m}$ is called a CP box of the order h ($1 \le h \le n$), if for arbitrary index set $i_1, i_2, ..., i_h$ and arbitrary index set $j_1, j_2, ..., j_h$ ($i_\alpha \ne i_\beta$ and $j_\alpha \ne j_\beta$ for $\alpha \ne \beta$) there is at least one vector V which specifies a permutation $\mathbf{P}_V$ moving x_{i_α} to y_{j_α} for all $\alpha = 1, 2, ..., h$.*

2 A Class of the Elementary Controlled Boxes

2.1 Design Criteria

The main building block in the layered CP boxes is the elementary switching element $\mathbf{P}_{2;1}$ performing controlled transposition of two input bits. The elementary controlled transformation performed with $\mathbf{P}_{2;1}$ is described by two specific Boolean functions (BFs) in three variables: $y_1 = f_1(x_1, x_2, v) = x_1 v \oplus x_2 v \oplus x_1$ and $y_2 = f_2(x_1, x_2, v) = x_1 v \oplus x_2 v \oplus x_2$, where x_1 and x_2 are the input bits, y_1 and y_2 are the output bits, and v is the controlling bit. Selecting the functions f_1 and f_2 of different types one can get different variants of the elementary controlled boxes $\mathbf{F}_{2;1}$ (see Figure 1). Using some given topology of the CP boxes and replacing the elements $\mathbf{P}_{2;1}$ by $\mathbf{F}_{2;1}$ one can get different variants of the controlled operational boxes performing transformations that in general case do not conserve the weight of the transformed binary vectors. Let such operational boxes be called the controlled operational substitutions (COSes).

The general structure of some layered $\mathbf{F}_{n;m}$-box is shown in Figure 2. It consist of $s = 2m/n$ active layers each of which contains $n/2$ parallel $\mathbf{F}_{2;1}$-boxes. A unique index is associated with each $\mathbf{F}_{2;1}$-box. For example, in Figure 2 all elementary boxes are consecutively numbered from left to right and from top to bottom. In accordance with such enumeration (indexing) the j-th bit of vector V controls the j-th elementary box $\mathbf{F}_{2;1}$ and the vector V can be represented as some concatenation of the $s = 2m/n$ vectors $V_1, V_2, ..., V_s \in \{0,1\}^{n/2}$, i.e. $V = (V_1, V_2, ..., V_s)$. Using different interconnections between active layers one can design different COS boxes for fixed variant of the box $\mathbf{F}_{2;1}$ and given values n and m. Such interconnections are denoted in Figure 2 as fixed permutations $\pi_1, ..., \pi_{k-1}$.

In general case a box $\mathbf{F}_{n;m}$ can be composed using elementary boxes $\mathbf{F}_{2;1}$ of several different types, i.e. each active layer can be unique. In this article we shall consider the COS boxes with uniform structure, i.e. the COS boxes built up from $\mathbf{F}_{2;1}$-boxes of the single type.

In many cases the use of the operation $\mathbf{F}_{n;m}$ while encrypting implies the use of its inverse $\mathbf{F}_{n;m}^{-1}$. It is evident, that arbitrary $\mathbf{F}_{n;m}$-box operation is invertible, if the elementary box $\mathbf{F}_{2;1}$ is invertible. Inverse transformation can

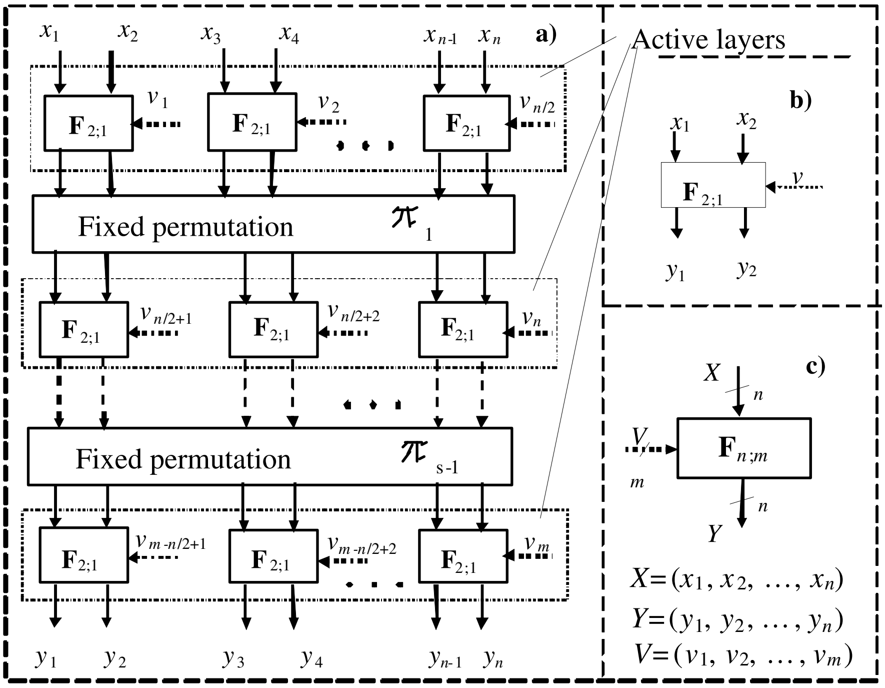
a)
b)
c)
Active layers
x_1 x_2 x_3 x_4 x_{n-1} x_n
$\mathbf{F}_{2;1}$
v_1 v_2 $v_{n/2}$
Fixed permutation π_1
$v_{n/2+1}$ $v_{n/2+2}$ v_n
Fixed permutation π_{s-1}
$v_{m-n/2+1}$ $v_{m-n/2+2}$ v_m
y_1 y_2 y_3 y_4 y_{n-1} y_n
x_1 x_2 v y_1 y_2
X n V m $\mathbf{F}_{n;m}$ Y
$X=(x_1, x_2, \dots, x_n)$
$Y=(y_1, y_2, \dots, y_n)$
$V=(v_1, v_2, \dots, v_m)$

Figure 2: The boxes $\mathbf{F}_{n;m}$: a – general structure, b – designation

be constructed by swapping input and output of the given COS box and replacing each of the elementary building boxes $\mathbf{F}_{2;1}$ by its inverse $\mathbf{F}_{2;1}^{-1}$. To define easy construction of the mutual inverse COS boxes one can propose to use the boxes $\mathbf{F}_{2;1}$ representing some elementary controlled involutions, i.e. the boxes both modifications $\mathbf{F}_0$ and $\mathbf{F}_1$ of which are involutions. The box $\mathbf{P}_{2;1}$ is one of them. Below we show that there exist 40 elementary controlled involutions and 24 of them are more interesting elementary cryptographic primitives than the $\mathbf{P}_{2;1}$-box.

If in the layered topology (see Figure 2) the elementary operation $\mathbf{F}_{2;1}$ is involution, then each active layer performs transformation of the n-bit strings, which is involution. In this case the inverse COS box is constructed by changing the fixed permutations and permuting the components V_1, V_2,...,V_s of the controlling vector as it is shown in Figure 3. Let the $\mathbf{F}_{2;1}$-boxes of some box $\mathbf{F}_{n;m}^{-1}$ be consecutively numbered from left to right and from bottom to top. Then in the mutually inverse COS boxes the jth controlling bit controls the jth elementary box.

Design of the COS boxes can be considered as a design at bit level. To formulate the criteria for selecting pairs of BFs^3 defining the $\mathbf{F}_{2;1}$-boxes suitable to the design of the COS boxes we have taken into account that the elementary switching box $\mathbf{P}_{2;1}$ is a main building block in the CP boxes and the last have been successfully used in the design of block ciphers [5]. Thus, we have formulated the following criteria arising from the main properties of $\mathbf{P}_{2;1}$:

C1. *Each of two outputs of the $\mathbf{F}_{2;1}$-box should be a non-linear* BF^3 *having maximum non-linearity.*

C2. *Each of two outputs of the $\mathbf{F}_{2;1}$-box should be a balanced* $\mathbf{BF}^3$.

C3. *Each of two elementary modifications of the $\mathbf{F}_{2;1}$-box, i.e. $\mathbf{F}_0$ and $\mathbf{F}_1$, should be bijective transformation $(x_1, x_2) \rightarrow (y_1, y_2)$.*

We have experimentally checked all of 256 existing BF^3 and have found 56 BFs satisfying criteria 1 and 2 (see Table 1). Our experiments based on exhaustive search have shown that there exist 288 pairs of BF^3 that define 288 different variants of the $\mathbf{F}_{2;1}$-boxes satisfying criteria C1, C2, and C3. Maximum non-linearity of the balanced BFs^n for odd n is $\mathrm{NL}_{\max}(f^n) = \lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \rfloor$ [18]. For non-linear BFs f^3 we have $\mathrm{NL}_{\max}(f(x_1, x_2, v)) = 2$. Note that non-linearity of each non-linear balanced BF^3 has value 2.

Having obtained comparatively large number of possible $\mathbf{F}_{2;1}$-boxes we have added new criteria that should help to select the best variants. Additional criteria are the following:

C4. *Linear combination of two outputs of the $\mathbf{F}_{2;1}$-box, i.e. the BF $f'(x_1, x_2, v) = y_1 \oplus y_2$, should be a non-linear BF^3 having maximum non-linearity.*

C5. *The $\mathbf{F}_{2;1}$-box should be a controlled involution, i.e. each of two its elementary modifications $\mathbf{F}_0$ and $\mathbf{F}_1$ should be involution.*

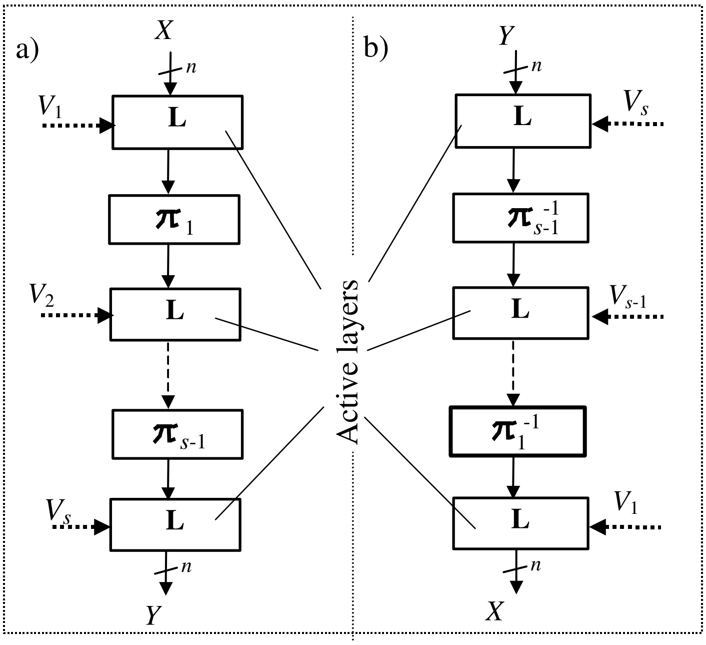

Figure 3: Mutually inverse COS boxes: a – $\mathbf{F}_{n;m}$, b – $\mathbf{F}_{n;m}^{-1}$

Criteria C1 to C4 define 192 different variants of the $\mathbf{F}_{2;1}$-boxes. The $\mathbf{P}_{2;1}$-box is beyond this set, since it does not satisfy criterion C4. Criteria C1 to C3 and C5 define 40 different variants of the $\mathbf{F}_{2;1}$-boxes two of them represent two variants of the elementary switching box (in literature the $\mathbf{P}_{2;1}^{(v)}$-box is described as that performing swapping two input bits at $v = 1$; the other variant $\mathbf{P}'_{2;1}$-box corresponds to swapping performed at $v = 0$). Criteria C1 to C5 define 24 (see Table 2) different variants of the elementary controlled involutions $\mathbf{F}_{2;1}$. Since the DDPs performed with the CP boxes represent an efficient cryptographic primitive one can conclude that the main design criteria are those that are satisfied by the $\mathbf{P}_{2;1}$-box, i.e. criteria C1 to C3. Criterion C4 should contribute significantly to the security of the COS-based ciphers. Meeting criterion C5 appears to be not necessary, but it is very useful for practical design of the COS boxes. Criterion C5 promotes easer design of the pairs of mutually inverse COS-box operations, for example CP boxes with symmetric topology can be transformed into its inverses by simple transposing of the components $V_1, V_2, ..., V_s$ of the controlling vector [5]. This possibility will be used in Section 4 while designing switchable COS boxes.

The box $\mathbf{P}_{2;1}$ does not satisfy criterion C4, i.e. sum of its outputs is a linear BF[3]: $y_1 \oplus y_2 = x_1 \oplus x_2$. The transformation defined by arbitrary $\mathbf{P}_{n;m}$-box conserves the weight of the input vector and for the CP boxes there exists one linear characteristic with bias 1/2 [5]. This defines necessity to combine CP-box operations with some other non-linear primitives while constructing encryption systems (see for example the ciphers CIKS-1 [11], SPECTR-H64 [6], and SPECTR-128 [5]).

The variants of the $\mathbf{F}_{2;1}$-boxes that satisfy criteria 1 to 4 define the substitution properties of the $\mathbf{F}_{n;m}$-boxes and possibility to design some pure COS-based ciphers, i.e. the ciphers that use only COS-box operations, fixed bit permutations, and the XOR operations. It is resonable to formulate also some avalanche criterion represented in one of the following two variants:

C6a. *Complementing one bit at input of the* $\mathbf{F}_{2;1}$*-box should define changing two output bits with probability 1/4.*

C6b. *Complementing one bit at input of the* $\mathbf{F}_{2;1}$*-box should define changing two output bits with probability 1/2.*

The $\mathbf{P}_{2;1}$-box does not satisfy any of these avalanche criteria. It is evident that no avalanche is introduced by any $\mathbf{P}_{n;m}$-box at fixed controlling vector, i.e. complementing one bit (let such bit be called active) at input of the $\mathbf{P}_{n;m}$-box defines changing only one output bit. Avalanche effect connected with the CP-box operations is caused by using each bit of the controlling data subblock to control several $\mathbf{P}_{2;1}$-boxes of the CP box [5, 11]. Thus, when performing a CP box operation the avalanche effect spreads only if the active bits are used as controlling ones. The COS boxes constructed on the basis of the $\mathbf{F}_{2;1}$-boxes satisfying the avalanche criterion C6a or C6b posses better avalanche properties, i.e. avalanche spreads also in the case when active bits pass through the COS box from input to output. One can expect that such $\mathbf{F}_{2;1}$-boxes allows one to design the COS-box operations providing some essential advantages against the CP boxes. One can show that if some $\mathbf{F}_{2;1}$-box satisfies criteria C1 to C4, then it satisfies also one of two criteria C6a and C6b. Thus, selection of the elementary controlled

Table 1: Full set of the BF^3 functions satisfying criteria C1 and C2 (the truth table of BF^3 are presented in the binary (1) and hexidecimal (2) forms)

1	2	1	2	1	2	1	2
00010111	17	00011011	1B	00011101	1D	00011110	1E
00100111	27	00101011	2B	00101101	2D	00101110	2E
00110101	35	00110110	36	00111001	39	00111010	3A
01000111	47	01001011	4B	01001101	4D	01001110	4E
01010011	53	01010110	56	01011001	59	01011100	5C
01100011	63	01100101	65	01101010	6A	01101100	6C
01110001	71	01110010	72	01110100	74	01111000	78
10000111	87	10001011	8B	10001101	8D	10001110	8E
10010011	93	10010101	95	10011010	9A	10011100	9C
10100011	A3	10100110	A6	10101001	A9	10101100	AC
10110001	B1	10110010	B2	10110100	B4	10111000	B8
11000101	C5	11000110	C6	11001001	C9	11001010	CA
11010001	D1	11010010	D2	11010100	D4	11011000	D8
1110001	E1	11100010	E2	11100100	E4	11101000	E8

boxes satisfying criteria C1 to C4 yields a new class of interesting cryptographic primitives. Criteria C6a and C6b serves to differentiate between two subclasses of such $\mathbf{F}_{2;1}$-boxes. Better avalanche and non-linearity of the sum of outputs provides possibility to construct a number of different COS boxes that are free of essential demerits of the CP boxes. From general point of view one can expect that using such advanced controlled operational boxes it is possible to design ciphers with fewer number of rounds reducing the hardware implementation cost and increasing performance. It seems also easier to construct the pure COS-based ciphers (one can propose some special design of the pure DDP-based cipher, however this is a topic of the individual research).

Let $\mathbf{F}_{2;1}$-boxes satisfying criteria C1 to C4, and C6b (C1 to C4, and C6a) be denoted as $\mathbf{S}_{2;1}$ ($\mathbf{R}_{2;1}$) and all the rest of the elementary boxes satisfying criteria C1 to C3 be denoted as $\mathbf{Z}_{2;1}$. We shall denote the COS boxes constructed using the elementary building blocks $\mathbf{S}_{2;1}$, $\mathbf{R}_{2;1}$, and $\mathbf{Z}_{2;1}$ as $\mathbf{S}_{n;m}$, $\mathbf{R}_{n;m}$, and $\mathbf{Z}_{n;m}$, correspondingly. Thus, we have the COS boxes of the **R**-type, **S**-type, and **Z**-type. The CP boxes belongs to the **Z**-type COS boxes.

2.2 Visual Design of the $\mathbf{F}_{2;1}$-boxes

Selection of the pairs of BF^3 considered above can be characterized as a formal selection of the $\mathbf{F}_{2;1}$-boxes with required properties. It allows to find all possible $\mathbf{F}_{2;1}$-boxes satisfying some given set of the design criteria, however some selected set of the BF^3 pairs can define the $\mathbf{F}_{2;1}$-boxes the difference between which is only formal and does not results in some essential differences of the properties of the constructed COS boxes. The box $\mathbf{F}_{2;1}^{(v)}$ defines two different modifications of the transformation $(x_1, x_2) \to (y_1, y_2)$: $\mathbf{F}_0$, if $v = 0$ and $\mathbf{F}_1$, if $v = 1$. Such transformations can be called elementary modifications. For formally different elementary boxes $\mathbf{F}_{2;1}$ and $\mathbf{F}'_{2;1}$ one can have $\mathbf{F}'_0 = \mathbf{F}_1$ and $\mathbf{F}'_1 = \mathbf{F}_0$.

Criterion C3 requires each of the modifications $\mathbf{F}_0$ and $\mathbf{F}_1$ be bijective. There exist only 24 variants of the bijective modifications $\mathbf{F}_v$. They are shown in Figure 4. One can propose some visual design of the $\mathbf{F}_{2;1}$-boxes which consists in selecting different pairs of the modifications from the set of possible ones. Note that each of the possible elementary modifications is a linear transformation. Non-linear properties of the $\mathbf{F}_{2;1}$-boxes are defined by specifying different elementary modifications to different values v. There are possible $24 \times 23 = 552$ ordered pairs and only 288 of them define non-linear $\mathbf{F}_{2;1}$-boxes satisfying criteria C1 to C3. Different variants of the representation of the $\mathbf{F}_{2;1}$-box as a pair of BFs^3 are shown in Figure 5.

After some pair of the modifications is selected as $\mathbf{F}_0$ and $\mathbf{F}_1$ one should write the BFs describing the $\mathbf{F}_{2;1}$-box and check if some chosen design criteria are satisfied. Boolean functions f_1 and f_2 describing some $\mathbf{F}_{2;1}$-box that is initially defined as a pair of the elementary modifications can be easy written in the following way. Let $\{f'_1(x_1, x_2),\ f'_2(x_1, x_2)\}$ be some pair of the BFs^2 describing the modification $\mathbf{F}_0$ that is assigned to value $v = 0$ and $\{f''_1(x_1, x_2), f''_2(x_1, x_2)\}$ be another pair of the BFs^2 describing the modification $\mathbf{F}_1$ that corresponds to $v = 1$. Then we have the following two BFs^3 describing the $\mathbf{F}_{2;1}$-box:

$$\begin{aligned} y_1 &= (v \oplus 1) f'_1(x_1, x_2) \oplus v f''_1(x_1, x_2), \\ y_2 &= (v \oplus 1) f'_2(x_1, x_2) \oplus v f''_2(x_1, x_2). \end{aligned}$$

For example, for the elementary box described by Figure 5a one can write:

$$\begin{aligned} y_1 &= (v \oplus 1)x_1 \oplus v x_2 = v x_1 \oplus v x_2 \oplus x_1, \\ y_2 &= (v \oplus 1)(x_1 \oplus x_2) \oplus v x_1 = v x_2 \oplus x_1 \oplus x_2, \end{aligned}$$

Table 2: Full set of the $\mathbf{F}_{2;1}$-boxes that are involutions satisfying criteria C1 to C5 (pairs of BF^3 are presented by pairs of truth tables in binary (1) and hexidecimal (2) representation)

#	1	2	#	1	2	#	1	2
1	00011011 00101101	$1B$ $2D$	9	00011011 10000111	$1B$ 87	17	00011110 00111001	$1E$ 39
2	00011110 10010011	$1E$ 93	10	00100111 00011110	27 $1E$	18	00100111 01001011	27 $4B$
3	00101101 00110110	$2D$ 36	11	00101101 01100011	$2D$ 63	19	00110110 00011011	36 $1B$
4	00111001 00100111	39 27	12	01001011 00111001	$4B$ 39	20	01001011 10010011	$4B$ 93
5	01001110 01111000	$4E$ 78	13	01001110 11010010	$4E$ $D2$	21	01100011 00011011	63 $1B$
6	01101100 01110010	$6C$ 72	14	10000111 00110110	87 36	22	10000111 01100011	87 63
7	10001101 10110100	$8D$ $B4$	15	10001101 11100001	$8D$ $E1$	23	10010011 00100111	93 27
8	10011100 10110001	$9C$ $B1$	16	11000110 01110010	$C6$ 72	24	11001001 10110001	$C9$ $B1$

$$y_1 \oplus y_2 \quad = \quad vx_1 \oplus x_2.$$

Using expression for y_1 and y_2 one can calculate the truth table and determine that Figure 5a defines the $\mathbf{F}_{2;1}$-box with number 1 in Table 2. After some practice it is easy to select the necessary pairs of the elementary modifications which define the boxes $\mathbf{F}_{2;1}$ satisfying the given set of criteria. Different variants of the $\mathbf{F}_{2;1}$-boxes constructed with such method are presented in Figure 5. Each of them satisfy the design criteria C1 to C3. Figures 5a to 5i show the $\mathbf{F}_{2;1}$-boxes that are elementary controlled involutions one of which is the elementary switching element $\mathbf{P}_{2;1}$ (Figure 5i). The $\mathbf{F}_{2;1}$-boxes corresponding to Figure 5a, 5c, 5d, and 5g satisfy criteria C1 to C5 and C6a. The $\mathbf{F}_{2;1}$-boxes corresponding to Figure 5b, 5e, 5f, and 5h satisfy criteria C1 to C5 and C6b. Figure 5 presents the most important types of the elementary boxes. The set of the $\mathbf{R}_{2;1}$-boxes includes several types of the elementary controlled involutions (see some examples in Figure 5). In frame of the visual design one can formulate one criterion more:

C7. *One of the $\mathbf{F}_{2;1}$-box modifications should include swapping bits.*

Use of this heuristic criterion allows one to attribute a subset of the $\mathbf{F}_{2;1}$-boxes to the class of the $\mathbf{P}_{2;1}$-like ones, which includes all boxes $\mathbf{R}_{2;1}$ (the set $\{\mathbf{R}_{2;1}\}$) and all boxes $\mathbf{Z}_{2;1}$ (the set $\{\mathbf{Z}_{2;1}\}$). For the elementary switching box we have $\mathbf{P}_{2;1} \in \{\mathbf{Z}_{2;1}\}$. There exists no $\mathbf{F}_{2;1}$-box that satisfies simultaneously the criteria C1 to C4, C6b, and C7, therefore no $\mathbf{P}_{2;1}$-like box is a $\mathbf{S}_{2;1}$-box. Let the COS boxes constructed from the $\mathbf{P}_{2;1}$-like elementary boxes be called CP-like or DDP-like ones. For the CP-like COS boxes it is reasonable to introduce the notion of the order:

Definition4. *The COS box $\mathbf{R}_{n;m}$ is called a COS box of the order h ($1 \leq h \leq n$), if it has the same topology as some CP box of the order h.*

The CP boxes $\mathbf{P}_{2^k;m}$ of the orders $h = 1, 2, ..., 2^{k-2}$, and 2^k can be implemented using s active layers, where s equals to $\log_2 n$, $\log_2 n + 1$,...,$2\log_2 n - 2$, and $2\log_2 n - 1$, respectively (the last figure corresponds also to implementation of the the CP box of the order 2^{k-1}) [5].

2.3 Classification of the $\mathbf{F}_{2;1}$-boxes

Representing the boxes $\mathbf{F}_{2;1}$ as pairs of the modifications $\mathbf{F}_0/\mathbf{F}_1$ it is easy to divide 192 variants satisfying criteria C1 to C4 into two sets $\{\mathbf{R}_{2;1}\}$ and $\{\mathbf{S}_{2;1}\}$. The first set includes all of 128 existing boxes $\mathbf{R}_{2;1}$ that satisfy additionally criterion C6a. The second set includes all of 64 existing boxes $\mathbf{S}_{2;1}$ that satisfy additionally criterion C6b. All boxes $\mathbf{Z}_{2;1}$ form the third set $\{\mathbf{Z}_{2;1}\}$ including 96 variants of the elementary controlled boxes which meet only criteria C1 to C3. Table 3 shows all representatives of these three sets. Each representative is shown as a pair of its two modifications $\mathbf{F}_0$ and $\mathbf{F}_1$. Rows in Tabe 5 correspond to the modification selected as $\mathbf{F}_0$ and columns correspond to modification $\mathbf{F}_1$. Letters R, S, and Z denote type of the $\mathbf{F}_{2;1}$-boxes.

Differential characteristics (DCs) of the COS boxes are defined by their topology and DCs of the elementary controlled boxes used as main building blocks while constructed the COS boxes. In general case the differences passing through the box $\mathbf{F}_{2;1}$ are shown in Figure 6. All boxes $\mathbf{S}_{2;1}$ posses the same DCs. All boxes $\mathbf{R}_{2;1}$ posses also the same DCs but different than that of the $\mathbf{S}_{2;1}$-boxes (see Table 4).

For all elementary boxes $\mathbf{Z}_{2;1}$ the sum $y_1 + y_2$ is a linear BF^3. Having investigated the DCs of all $\mathbf{Z}_{2;1}$-boxes we have divided them into four subsets:

1) The subset $\{\dot{\mathbf{Z}}_{2;1}\}$ includes 32 elementary controlled boxes satisfying criteria C6a and defining the probability $\Pr(\Delta_1^Y/\Delta_0^X, \Delta_1^V) = 1$.

2) The subset $\{\ddot{\mathbf{Z}}_{2;1}\}$ includes 32 elementary controlled boxes satisfying criteria C6a and defining the probability $\Pr(\Delta_2^Y/\Delta_0^X, \Delta_1^V) = 1/2$.

3) The subset $\{\tilde{\mathbf{Z}}_{2;1}\}$ includes 16 elementary controlled boxes defining the probabilities $\Pr(\Delta_1^Y/\Delta_1^X, \Delta_0^V) = 1$ and $\Pr(\Delta_1^Y/\Delta_0^X, \Delta_1^V) = 1$.

4) The subset $\{\mathbf{Z}'_{2;1}\}$ includes 16 elementary controlled boxes defining the probabilities $\Pr(\Delta_1^Y/\Delta_1^X, \Delta_0^V) = 1$ and $\Pr(\Delta_2^Y/\Delta_0^X, \Delta_1^V) = 1/2$.

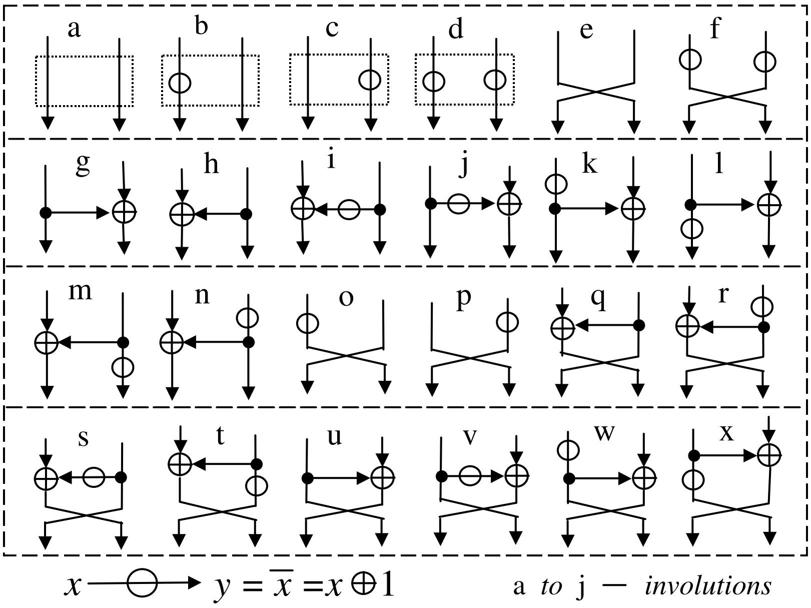

Figure 4: The set of the existing elementary modifications of the $\mathbf{F}_{2;1}$-boxes

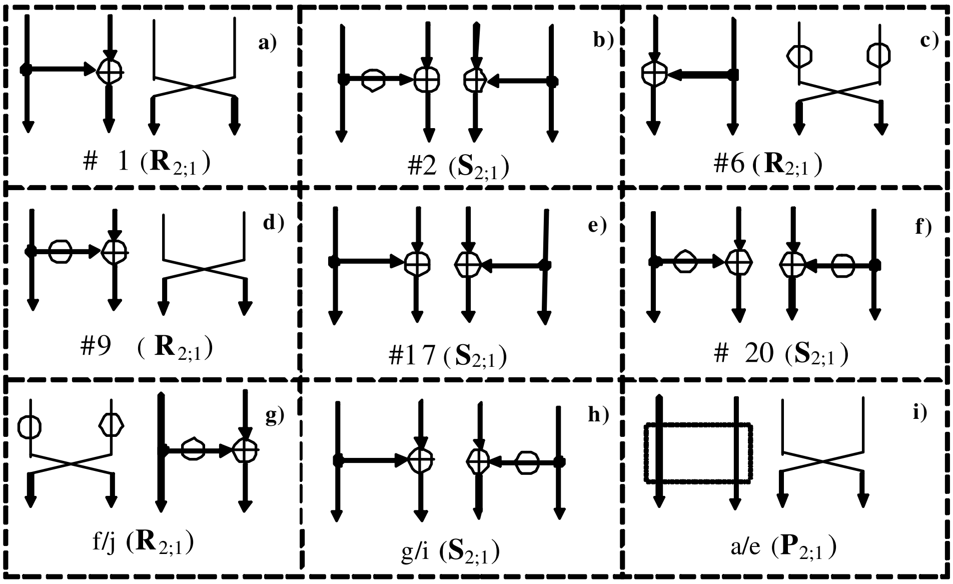

Figure 5: Some elementary boxes $\mathbf{F}_{2;1}$ defined as pairs of the elementary modifications

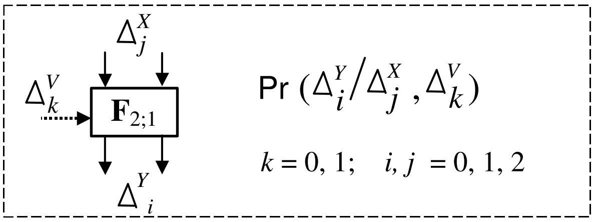
Δ_j^X
Δ_k^V
$\mathbf{F}_{2;1}$
Δ_i^Y
$\Pr(\Delta_i^Y/\Delta_j^X, \Delta_k^V)$
$k = 0, 1; \quad i, j = 0, 1, 2$

Figure 6: Designation of the differences corresponding to the elementary boxes $\mathbf{F}_{2;1}$

Table 3: Possible types of the $\mathbf{F}_{2;1}$-boxes satisfying criteria C1 to C3

F0\F1	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
a	-				P	Z'									$\tilde{Z}$	Z'	R	R	R	R	R	R	R	R
b		-			$\tilde{Z}$	$\tilde{Z}$									Z'	$\tilde{Z}$	R	R	R	R	R	R	R	R
c			-		$\tilde{Z}$	$\tilde{Z}$									$\tilde{Z}$	Z'	R	R	R	R	R	R	R	R
d				-	Z'	Z'									Z'	$\tilde{Z}$	R	R	R	R	R	R	R	R
e	P$'$	$\tilde{Z}$	$\tilde{Z}$	Z'	-		R	R	R	R	R	R	R	R										
f	Z'	$\tilde{Z}$	$\tilde{Z}$	Z'		-	R	R	R	R	R	R	R	R										
g					R	R	-	S	S				S	S	R	R					$\ddot{Z}$	$\dot{Z}$	$\ddot{Z}$	$\dot{Z}$
h					R	R	S	-		S	S	S			R	R	$\ddot{Z}$	$\ddot{Z}$	$\dot{Z}$	$\dot{Z}$				
i					R	R	S		-	S	S	S			R	R	$\dot{Z}$	$\dot{Z}$	$\ddot{Z}$	$\ddot{Z}$				
j					R	R		S	S	-			S	S	R	R					$\dot{Z}$	$\ddot{Z}$	$\dot{Z}$	$\ddot{Z}$
k					R	R		S	S		-		S	S	R	R					$\ddot{Z}$	$\dot{Z}$	$\ddot{Z}$	$\dot{Z}$
l					R	R		S	S			-	S	S	R	R					$\dot{Z}$	$\ddot{Z}$	$\dot{Z}$	$\ddot{Z}$
m					R	R	S			S	S	S	-		R	R	$\dot{Z}$	$\dot{Z}$	$\ddot{Z}$	$\ddot{Z}$				
n					R	R	S			S	S	S		-	R	R	$\ddot{Z}$	$\ddot{Z}$	$\dot{Z}$	$\dot{Z}$				
o	$\tilde{Z}$	Z'	$\tilde{Z}$	Z'			R	R	R	R	R	R	R	R	-									
p	Z'	$\tilde{Z}$	Z'	$\tilde{Z}$			R	R	R	R	R	R	R	R		-								
q	R	R	R	R				$\ddot{Z}$	$\dot{Z}$				$\dot{Z}$	$\ddot{Z}$			-				S	S	S	S
r	R	R	R	R				$\ddot{Z}$	$\dot{Z}$				$\dot{Z}$	$\ddot{Z}$				-			S	S	S	S
s	R	R	R	R				$\dot{Z}$	$\ddot{Z}$				$\ddot{Z}$	$\dot{Z}$					-		S	S	S	S
t	R	R	R	R				$\dot{Z}$	$\ddot{Z}$				$\ddot{Z}$	$\dot{Z}$						-	S	S	S	S
u	R	R	R	R			$\ddot{Z}$			$\dot{Z}$	$\ddot{Z}$	$\dot{Z}$					S	S	S	S	-			
v	R	R	R	R			$\dot{Z}$			$\ddot{Z}$	$\dot{Z}$	$\ddot{Z}$					S	S	S	S		-		
w	R	R	R	R			$\ddot{Z}$			$\dot{Z}$	$\ddot{Z}$	$\dot{Z}$					S	S	S	S			-	
x	R	R	R	R			$\dot{Z}$			$\ddot{Z}$	$\dot{Z}$	$\ddot{Z}$					S	S	S	S				-

The elementary switching box $\mathbf{P}_{2;1}$ is an element of the subset $\{\mathbf{Z}'_{2;1}\}$: $\mathbf{P}_{2;1} \in \{\mathbf{Z}'_{2;1}\}$. Some probabilistic properties of the subsets are presented in Table 4. One can see that the boxes $\mathbf{S}_{2;1}$ and $\mathbf{R}_{2;1}$ are less predictable than the boxes $\mathbf{Z}_{2;1}$. Proposed classification define the following properties:

1) If $\mathbf{F}_{2;1} \in \{\mathbf{S}_{2;1}\}$, then $\mathbf{F}^{-1}_{2;1} \in \{\mathbf{S}_{2;1}\}$.

2) If $\mathbf{F}_{2;1} \in \{\mathbf{R}_{2;1}\}$, then $\mathbf{F}^{-1}_{2;1} \in \{\mathbf{R}_{2;1}\}$.

3) If $\mathbf{F}_{2;1} \in \{\tilde{\mathbf{Z}}_{2;1}\} \cup \{\mathbf{Z}'_{2;1}\}$, then $\mathbf{F}^{-1}_{2;1} \in \{\tilde{\mathbf{Z}}_{2;1}\} \cup \{\mathbf{Z}'_{2;1}\}$. If the boxes $\tilde{\mathbf{Z}}_{2;1}$ and $\mathbf{Z}'_{2;1}$ are not involutions, then $\tilde{\mathbf{Z}}^{-1}_{2;1} \in \{\mathbf{Z}'_{2;1}\}$ and $\mathbf{Z}'^{-1}_{2;1} \in \{\tilde{\mathbf{Z}}_{2;1}\}$.

4) If $\mathbf{F}_{2;1} \in \{\dot{\mathbf{Z}}_{2;1}\} \cup \{\ddot{\mathbf{Z}}_{2;1}\}$, then $\mathbf{F}^{-1}_{2;1} \notin \{\mathbf{Z}_{2;1}\} \cup \{\mathbf{S}_{2;1}\} \cup \{\mathbf{R}_{2;1}\}$, since one of two outputs of such $\mathbf{F}^{-1}_{2;1}$-boxes is a linear BF^3.

Among 288 boxes $\mathbf{F}_{2;1}$ we have 40 involutions: 8 involutions $\mathbf{S}_{2;1}$, 16 involutions $\mathbf{R}_{2;1}$, and 16 involutions $\mathbf{Z}_{2;1}$. The last two subsets represent 32 $\mathbf{P}_{2;1}$-like elementary controlled involutions. All elementary controlled involutions $\mathbf{F}_{2;1}$ are presented in the upper-left part of Table 3. Twenty four involutions corresponding to the set $\{\mathbf{S}_{2;1}\} \cup \{\mathbf{R}_{2;1}\}$ are presented in Table 2 as pairs of BFs^3. The involutions included in this set are the most attractive ones for the use in the design of the COS-box operations.

3 Controlled Operational Substitutions

Design of the operational boxes $\mathbf{R}_{n;m}$ and $\mathbf{S}_{n;m}$ includes the following two items: (1) selection of the fixed permutations between active layers and (2) selection of the types of active layers. The topologies developed for the CP boxes of different orders [5] present different variants of the sets of fixed permutations suitable to construction COS boxes. The second item is a new one against the $\mathbf{P}_{n;m}$-boxes design. Using different variants of the $\mathbf{F}_{2;1}$-boxes one can design different variants of the active layers. Even in a single COS box different active layers can be used. One can consider the following approaches to the COS-box design:

1) Use of the $\mathbf{F}_{2;1}$-boxes of the same type.

2) Use of the active layers of different types, each single active layer being constructed with the $\mathbf{F}_{2;1}$-boxes of the same type.

3) Use of the active layers of the same type, the active layers comprising different types of the $\mathbf{F}_{2;1}$-boxes.

4) Arbitrary use of different types of the elementary controlled boxes.

The first approach allows one to design COS boxes having more uniform structure providing easier calculation of their properties. In the frame of the first approach

Table 4: Values of the probability $\Pr(\Delta_i^Y/\Delta_j^X, \Delta_k^V)$ for different types of the $\mathbf{F}_{2;1}$-boxes

i	j	k	$\mathbf{S}_{2;1}$	$\mathbf{R}_{2;1}$	$\dot{\mathbf{Z}}_{2;1}$	$\ddot{\mathbf{Z}}_{2;1}$	$\tilde{\mathbf{Z}}_{2;1}$	$\mathbf{Z}'_{2;1}$
0	0	1	1/4	1/4	0	1/2	0	1/2
1	0	1	1/2	1/2	1	0	1	0
2	0	1	1/4	1/4	0	1/2	0	1/2
0	1	1	1/4	1/4	1/4	1/4	1/2	0
1	1	1	1/2	1/2	1/2	1/2	0	1
2	1	1	1/4	1/4	1/4	1/4	1/2	0
1	1	0	1/2	3/4	1/2	1/2	1	1
2	1	0	1/2	1/4	1/2	1/2	0	0
1	2	0	1	1/2	1	1	0	0
2	2	0	0	1/2	0	0	1	1
0	2	1	1/4	1/4	1/2	0	0	1/2
1	2	1	1/2	1/2	0	1	1	0
2	2	1	1/4	1/4	1/2	0	0	1/2
Examples, $\mathbf{F}_0/\mathbf{F}_1$			h/g; j/i m/g; u/t	g/e; i/f p/h; x/d	l/u; k/x n/s; j/u	l/v; l/s n/r; j/x	b/e; c/f a/o; d/p	a/f; e/a b/o; c/p

it is more interesting to use elementary controlled involutions $\mathbf{R}_{n;m}$ and $\mathbf{S}_{n;m}$, since in different cryptoschemes one should use mutually inverse operations. Let us construct a $\mathbf{S}_{n;m}$ box, containing $\log_2 n$ active layers and having parameters $n = 2^k$ and $m = kn/2$, where $k \geq 2$ is a natural number.The fixed permutation between jth and $(j+1)$th active layers we define as follows. For $g = 1, 2, ..., n/2$ the $(2g-1)$th output of the jth active layer is connected with the $(2g-1)$th input of the $(j+1)$th active layer. The $2g$th output of the jth active layer is connected with the ith input of the $(j+1)$th active layer, where

$$i = \begin{cases} 2g + 2^j, & \text{if } g \leq g_0 = \frac{n}{2} - 2^{j-1}; \\ 2g + 2^j - n, & \text{if } \frac{n}{2} - 2^{j-1} < g \leq \frac{n}{2}. \end{cases} \quad (1)$$

Thus, the fixed permutations corresponding to $j = 1, 2, ..., k-1$ are described by the following table:

1	2	3	$\cdots$	$2g$	$\cdots$
1	$2+2^j$	3	$\cdots$	$n-2^j$	$\cdots$
$2g_0$	$\cdots$	$2g$	$\cdots$	$n-1$	n
n	$\cdots$	$2g+2^j-n$	$\cdots$	$n-1$	2^j

It is evident the $\mathbf{R}$-type COS boxes having topology described by Formula (1) are of the first order. The COS boxes $\mathbf{F}_{8;12}$ and $\mathbf{F}_{16;32}$, where $\mathbf{F} \in \{\mathbf{R}, \mathbf{S}\}$, constructed with the use of such fixed permutations are shown in Figure 7. It is easy to show that for such COS boxes each output is some BF in μ variables, where $\mu = 2n-1 = 2^{k+1}-1$. Indeed, the output y_i, $i = 1, 2, ..., n$, depends on one controlling bit corresponding to the sth layer ($s = 2m/n = \log_2 n$) and on two outputs of the $(s-1)$th layer. Each of the lasts depends on one controlling bit corresponding to the $(s-1)$th layer and two output bits of the $(s-2)$th layer. Considering consecutively all other layers one can calculate that y_i depends on all input bits and z controlling bits, where $z = 1+2+...+2^{k-1} = 2^k - 1$, i.e. we have $z + n = \mu$. Taking into account that BFs^3 describing the elementary boxes $\mathbf{R}_{2;1}$ and $\mathbf{S}_{2;1}$ have the algebraic degree 2 it is easy to calculate that for all i the algebraic degree of the BF$^\mu$ describing the output y_i is equal to $k+1$.

Since each output bit of the $\mathbf{F}_{n;m}$-box is some BF in $\mu = 2n-1$ variables one can describe the $\mathbf{F}_{n;m}$-box as some set Φ of the component BFs$^\mu$. To estimate nonlinearity of some $f_i^\mu \in \Phi$ one can use the Formula [18]:

$$\mathrm{NL}(f_i^\mu) = 2^{n-1} - \frac{1}{2} \max_{\forall \alpha \in GF(2)^n} \left| \hat{U}_\alpha(f_i^\mu) \right|, \quad (2)$$

where $\hat{U}_\alpha(f_i^\mu)$ is the value of the Walsh-Hadamard spectrum component corresponding to vector α.

For $n \leq 8$ we have experimentally investigated WHT of all component BFs$^\mu$ of the $\mathbf{F}_{n;m}$-boxes constructed from elementary controlled involutions $\mathbf{S}_{2;1}$ or $\mathbf{R}_{2;1}$ presented in Table 2. The experiment has shown that the maximum value of the WHT component is described by the formula

$$\max_{\forall \alpha \in GF(2)^n} \left| \hat{U}_\alpha(f_i^\mu) \right| = \frac{2^\mu}{n} = \frac{2^{2n-1}}{n} = 2^{2^{k+1}-k-1}. \quad (3)$$

This result can be interpreted as follows. In each layer two outputs of each elementary box represent balanced BFs related to the same class. One can represent the (x_1, x_2) input of arbitrary box $\mathbf{F}_{2;1}$ in the next (for example, in the second) active layer as the Kroneker product of the BFs f_1 and f_2 with the row-vector $||11...1||$, i.e. $x_1 = f_1 \otimes ||11...1||^T$ and $x_2 = ||11...1|| \otimes f_2^T$, where the number of elements in the row-vector is equal to the number of elements of the truth table of BFs. Due to recursive construction of the Hadamard's matrices the increase of the number of variables in the component BFs of the $\mathbf{F}_{n;m}$-box does not change the features of the WHT spectrum of the component BFs. For elementary box $\mathbf{S}_{2;1}$ we have $\mu = 3$, $n = 2$, and $\max_{\forall \alpha \in GF(2)^n} \left| \hat{U}_\alpha(f_i^\mu) \right| = \frac{2^\mu}{n}$, therefore this dependence is conserved for all component

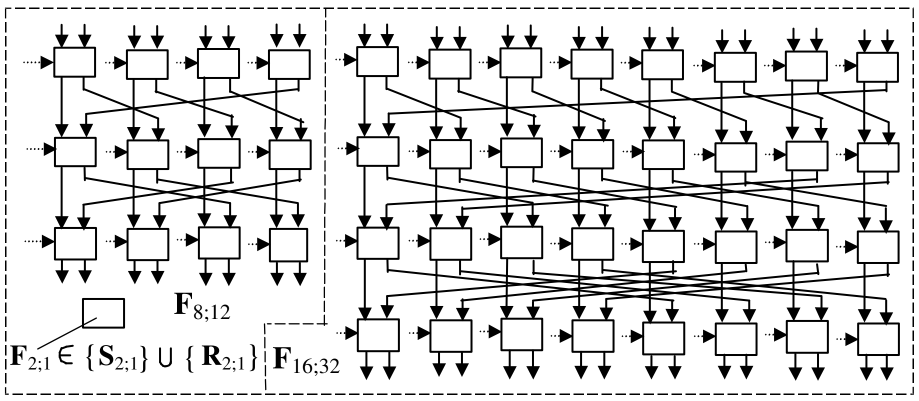
$\mathbf{F}_{8;12}$
$\mathbf{F}_{2;1} \in \{\mathbf{S}_{2;1}\} \cup \{\mathbf{R}_{2;1}\}$
$\mathbf{F}_{16;32}$

Figure 7: Examples of the COS boxes: a – $\mathbf{R}_{8;12}$ and $\mathbf{S}_{8;12}$, b – $\mathbf{R}_{16;32}$ and $\mathbf{S}_{16;32}$

BFs implementing the $\mathbf{F}_{n;m}$-box. Thus, the experimental results and their interpretation give us grounds to put forward the following hypothesis.

Hypothesis 1. *Let the COS box $\mathbf{F}_{n;m}$ be constructed using the elementary building blocks $\mathbf{F}_{2;1}$ presented in Table 4 and topology described by* (1). *Then maximum value of the WHT component of each component BF$^{\mu}$ is described by Formula* (3).

From Formulas (2) and (3) one can obtain the following formula for estimating the non-linearity of the component BFs of the $\mathbf{R}_{n;m}$- and $\mathbf{S}_{n;m}$-boxes:

$$\mathrm{NL}(f_i^{\mu}) = 2^{\mu-1} - \frac{2^{\mu-1}}{n} = \frac{2^{2n-2}(n-1)}{n} = (n-1)2^{2n-k-2}.$$

The non-linearity of arbitrary BF$^{\mu}$ has the following theoretic limitation [18]:

$$\mathrm{NL}(f^{\mu}) \leq 2^{\mu-1} - 2^{\frac{\mu}{2}-1}.$$

Only bent functions $f_{\mathrm{bent}}^{\mu'}$ have maximum non-linearity $\mathrm{NL}_{\max}(f^{\mu'}) = \mathrm{NL}(f_{\mathrm{bent}}^{\mu'}) = 2^{\mu'-1} - 2^{\frac{\mu'}{2}-1}$, where μ' is even. For arbitrary balanced BF f_{bal}^{μ}, where μ is even or odd, we have $\mathrm{NL}_{\max}(f_{\mathrm{bal}}^{\mu}) < 2^{\mu-1} - 2^{\frac{\mu}{2}-1} - 2$ [18]. For all component BFs f_i^{μ} of the investigated COS boxes we have the following ratio

$$\frac{\mathrm{NL}(f_i^{\mu})}{\mathrm{NL}_{\max}(f_{\mathrm{bal}}^{\mu})} > \frac{2^{\mu-1} - \frac{2^{\mu-1}}{n}}{2^{\mu-1} - 2^{\frac{\mu}{2}-1}} = \frac{1-\frac{1}{n}}{1-2^{-\frac{\mu}{2}}} = \frac{1-\frac{1}{n}}{1-2^{-n+\frac{1}{2}}}. \quad (4)$$

Thus, non-linearity of all component BFs is close to the maximal possible non-linearity of the balanced BFs in μ variables. The ratio (4) tends to value 1 while increasing n, the difference $\mathrm{NL}_{\max}(f_{\mathrm{bal}}^{\mu}) - \mathrm{NL}(f_i^{\mu}) = 2^k(2^{\frac{1}{2}} - 1)$ increases also though.

For $n = 4, 8, 16$ we have experimentally investigated the autocorrelation function $r_{\alpha}(f) = \frac{1}{2^{\mu}} \sum_{X' \in GF(2)^{\mu}} (-1)^{f(X') \oplus f(X' \oplus \alpha)}$, where $X', \alpha \in GF(2)^{\mu}$, of all component BFs $f_i^{\mu}(X')$ of different variants $\mathbf{S}_{n;m}$-boxes constructed using different elementary controlled involutions $\mathbf{S}_{2;1}$ (see Table 5) and topology described by Formula (1). We have obtained that $r_{\alpha}(f) = 0$ for $2^{\mu} - 1$ vectors $\alpha \in GF(2)^{\mu}$. This shows that all component BFs $f_i^{\mu}(X') \in \Phi$ have good propagation properties.

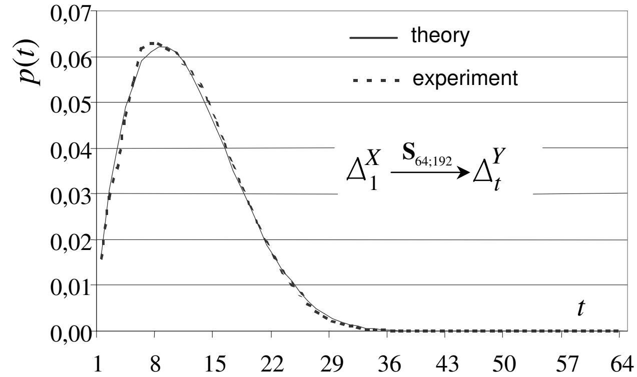

Figure 8: Probability distribution $p(t) = \Pr(\Delta_t^Y / \Delta_1^X, \Delta_0^V)$ for the $\mathbf{S}_{64;192}$-box

Using data of Table 4 and technique of the probability generating functions we have calculated the $\Pr(\Delta_t^Y / \Delta_1^X, \Delta_0^V)$ probability of the transformation of the input difference Δ_1^X with the weight 1 into the output differences Δ_t^Y with the weight t, while passing through the $\mathbf{S}_{64;192}$-box. For each value t the same probability has been obtained for the $\mathbf{S}_{64;192}$-boxes constructed from different elementary building boxes $\mathbf{S}_{2;1}$ presented in Table 5. The results of the calculation are presented in Table 6. Then we have performed statistic experiments to determine the experimental values of the probabilities $\Pr(\Delta_t^Y / \Delta_1^X, \Delta_0^V)$. The experimental and theoretic curves of the probability distribution $p(t) = \Pr(\Delta_t^Y / \Delta_1^X, \Delta_0^V)$ are in a good agreement (see Figure 8). Thus, the $\mathbf{S}_{64;192}$-box posses significantly better difference propagation properties than the box $\mathbf{P}_{64;192}$. Indeed, for arbitrary CP box we have $\Pr(\Delta_1^Y / \Delta_1^X, \Delta_0^V) = 1$.

Table 5: The set of the involutions $\mathbf{S}_{2;1}$

#	Elementary modifications		Algebraic normal forms of BF	
	$\mathbf{F}_0$	$\mathbf{F}_1$	f_1	f_2
15	g	h	$x_2v \oplus x_1$	$x_1v \oplus x_1 \oplus x_2$
21	j	h	$x_2v \oplus x_1$	$x_1v \oplus x_1 \oplus x_2 \oplus v \oplus 1$
39	h	g	$x_2v \oplus x_1 \oplus x_2$	$x_1v \oplus x_2$
42	h	j	$x_2v \oplus x_1 \oplus x_2$	$x_1v \oplus x_2 \oplus v$
75	g	i	$x_2v \oplus x_1 \oplus v$	$x_1v \oplus x_1 \oplus x_2$
81	j	i	$x_2v \oplus x_1 \oplus v$	$x_1v \oplus x_1 \oplus x_2 \oplus v \oplus 1$
147	i	g	$x_2v \oplus x_1 \oplus x_2 \oplus v \oplus 1$	$x_1v \oplus x_2$
150	i	j	$x_2v \oplus x_1 \oplus x_2 \oplus v \oplus 1$	$x_1v \oplus x_2 \oplus v$

4 Some Items of The COS-based Cipher Design

4.1 Switchable Controlled Operations

The COS-based design of the ciphers represents a variant of the bit-level design that suits well to develop fast cryptosystems oriented to the low-cost hardware implementation. The COS boxes are more efficient as compared with the CP boxes, since (1) they change arbitraly the weight of the input vector, (2) they define significant avalanche while data are transformed with them, (3) they define lower probability that the low-weight differences of the controlling vector do not introduce changes in the output, and (4) the sum of all outputs of the COS boxes is a non-linear BF versus linearity of such sum in the case of the CP boxes. Since different examples of the cipher design based on using the CP-box operations have shown DDPs' efficiency as cryptographic primitive [5], one can expect that replacing the CP boxes in the already proposed ciphers by the COS boxes one can provide possibility to reduce the number of the encryption rounds. For many hardware implementation architectures this results in higher performance and lower implementation cost.

Data-dependent operations are very attractive to be used together with simple key scheduling. However the use of the simple key scheduling introduces the problem of weak keys. This problem is especially important while designing hash functions with the use of block ciphers.

Definition 5. *Let $\mathbf{F}'^{(e)}$, where $e \in \{0,1\}$, be some e-dependent operation containing two modifications $\mathbf{F}'^{(0)} = \mathbf{F}'_0$ and $\mathbf{F}'^{(1)} = \mathbf{F}'_1$, where $\mathbf{F}'_1 = \mathbf{F}'^{-1}_0$. Then the operation $\mathbf{F}'^{(e)}$ is called switchable.*

Definition 6. *Let two modifications of the switchable operation $\mathbf{F}'^{(e)}$ be mutual inverses $\mathbf{F}'^{(0)} = \mathbf{F}^{(V)}$ and $\mathbf{F}'^{(1)} = (\mathbf{F}^{-1})^{(V)}$. Then $\mathbf{F}'^{(e)}$ is called switchable controlled operation $\mathbf{F}^{(V,e)}$.*

Below we describe the switchable COS boxes $\mathbf{R}^{(V,e)}_{32;96}$ and $\mathbf{R}^{(V,e)}_{64;192}$ representing practical interest in the design of the 64- and 128-bit ciphers, correspondingly. Such switchable operational boxes are constructed on the bases of the COS boxes $\mathbf{R}_{32;96}$ and $\mathbf{R}_{64;192}$ with symmetric structure. These boxes can be constructed using the single-type elementary controlled involutions represented, for example, by one of the following pairs of BFs^3 #9, #19, #6, and #24 (see Table 2). The boxes $\mathbf{R}_{8;12}$ (Figure 9a) and $\mathbf{R}^{-1}_{8;12}$ (Figure 9b) containing three active layers are used as main building blocks while constructing the six-layer boxes $\mathbf{R}_{32;96}$ (Figure 9c) and $\mathbf{R}_{64;192}$ (Figure 9e). It is easy to show the $\mathbf{R}_{32;96}$ and $\mathbf{R}_{64;192}$ are the boxes of the second and first orders, correspondingly.

The fixed permutation π_3 corresponding to connections between four parallel boxes $\mathbf{R}_{8;12}$ and four parallel boxes $\mathbf{R}^{-1}_{8;12}$ in $\mathbf{R}_{32;96}$-box is described as the following fixed permutational involution $\mathbf{I}_1$:

(1)(2,9)(3,17)(4,25)(5)(6,13)(7,21)(8,29)(10)(11,18)
(12,26)(14)(15,22)(16,30)(19)(20,27)(23)(24,31)(28)(32).

The fixed permutation π'_3 corresponding to connections between eight parallel boxes $\mathbf{R}_{8;12}$ and eight parallel boxes $\mathbf{R}^{-1}_{8;12}$ in $\mathbf{R}_{64;192}$-box represents the following permutational involution $\mathbf{I}_2$:

(1)(2,9)(3,17)(4,25)(5,33)(6,41)(7,49)(8,57)(10)(11,18)
(12,26)(13,34)(14,42)(15,50)(16,58)(19)(20,27)(21,35)
(22,43)(23,51)(24,59)(28)(29,36)(30,44)(31,52)(32,60)(37)
(38,45)(39,53)(40,61)(46)(47,54)(48,62)(55)(56,63)(64).

Due to symmetric topology the difference between the boxes $\mathbf{R}_{32;96}$ (Figure 9c) and $\mathbf{R}^{-1}_{32;96}$ (Figure 7d) consists only in the use of the controlling-vector components V_1, V_2,...,V_6. Between the boxes $\mathbf{P}_{64;192}$ (Figure 9e) and $\mathbf{R}^{-1}_{64;192}$ (Figure 9f) we have analogous difference. Due to symmetric topology the modifications $\mathbf{R}_V$, where $V = (V_1, V_2, ...V_6)$, and $\mathbf{R}_{V'}$, where $V' = (V_6, V_5..., V_1)$ are mutually inverse. Such property is a core one for the design of the switchable COS boxes $\mathbf{R}^{(V,e)}_{64;192}$ and $\mathbf{R}^{(V,e)}_{32;96}$. Thus, reversing the order of the use of the components V_1, V_2,...,V_s in arbitrary symmetric COS box one can define switching between two mutually inverse boxes $\mathbf{R}_{n;m}$ and $\mathbf{R}^{-1}_{n;m}$.

The box $\mathbf{R}^{(V,e)}_{32;96}$ can be constructed using very simple transposition box $\mathbf{P}^{(e)}_{96;1}$ implemented as some single-layer CP box comprising three parallel single-layer boxes

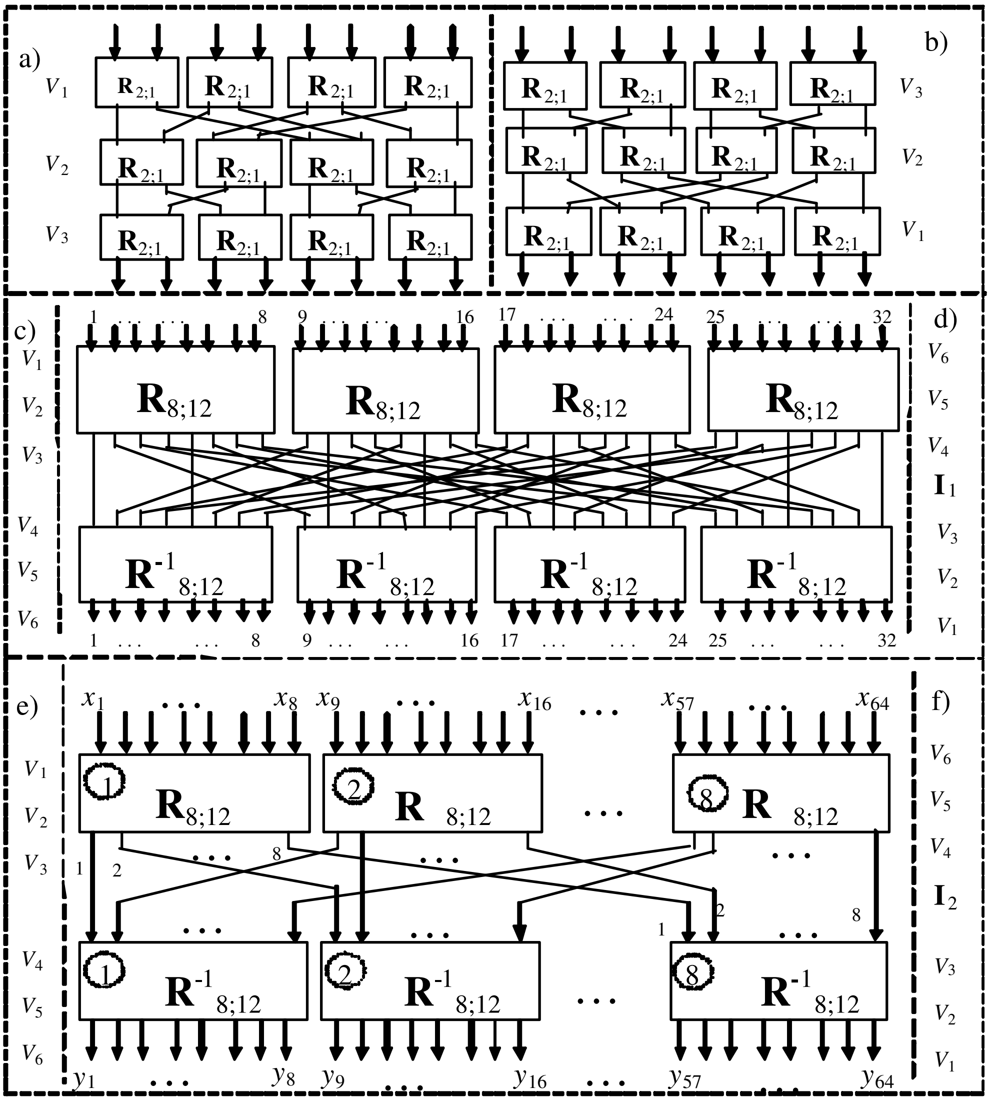

Figure 9: Mutually inverse COS boxes with symmetric topology: a – $\mathbf{R}_{8;12}$, b – $\mathbf{R}^{-1}_{8;12}$, c – $\mathbf{R}_{32;96}$, d – $\mathbf{R}^{-1}_{32;96}$, e – $\mathbf{R}_{64;192}$, f – $\mathbf{R}^{-1}_{64;192}$

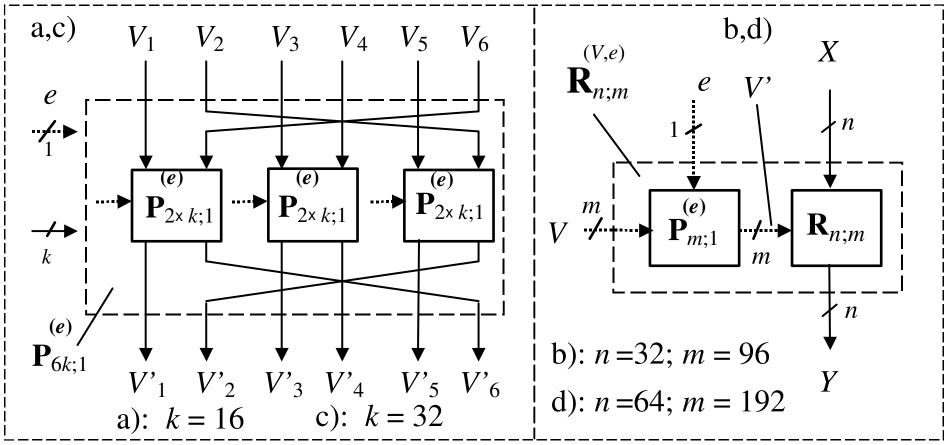
a,c)
V_1 V_2 V_3 V_4 V_5 V_6
e
1
k
$\mathbf{P}^{(e)}_{2\times k;1}$
$\mathbf{P}^{(e)}_{6k;1}$
V'_1 V'_2 V'_3 V'_4 V'_5 V'_6
a): $k = 16$
c): $k = 32$
b,d)
$\mathbf{R}^{(V,e)}_{n;m}$
e
V'
X
n
V
m
$\mathbf{P}^{(e)}_{m;1}$
$\mathbf{R}_{n;m}$
Y
b): n =32; m = 96
d): n =64; m = 192

Figure 10: Construction of the switchable COS boxes: a – $\mathbf{P}^{(e)}_{96;1}$-box, b – $\mathbf{R}^{(V,e)}_{32;96}$-box, c – $\mathbf{P}^{(e)}_{192;1}$-box, d – $\mathbf{R}^{(V,e)}_{64;192}$-box

Table 6: Theoretic values of the probability $\Pr(\Delta_t^Y/\Delta_1^X, \Delta_0^V)$ for the $\mathbf{S}_{64;192}$-box

t	p	t	p	t	p	t	p
1	$1.6 \cdot 10^{-2}$	17	$3.5 \cdot 10^{-2}$	33	$6.6 \cdot 10^{-4}$	49	$2.3 \cdot 10^{-8}$
2	$3.1 \cdot 10^{-2}$	18	$3.1 \cdot 10^{-2}$	34	$4.4 \cdot 10^{-4}$	50	$8.6 \cdot 10^{-9}$
3	$4 \cdot 10^{-2}$	19	$2.7 \cdot 10^{-2}$	35	$2.8 \cdot 10^{-4}$	51	$3 \cdot 10^{-9}$
4	$4.9 \cdot 10^{-2}$	20	$2.3 \cdot 10^{-2}$	36	$1.8 \cdot 10^{-4}$	52	$1 \cdot 10^{-9}$
5	$5.4 \cdot 10^{-2}$	21	$1.9 \cdot 10^{-2}$	37	$1.1 \cdot 10^{-4}$	53	$3.1 \cdot 10^{-10}$
6	$5.9 \cdot 10^{-2}$	22	$1.96 \cdot 10^{-2}$	38	$6.6 \cdot 10^{-5}$	54	$8.8 \cdot 10^{-11}$
7	$6.1 \cdot 10^{-2}$	23	$1.3 \cdot 10^{-2}$	39	$3.8 \cdot 10^{-5}$	55	$2.3 \cdot 10^{-11}$
8	$6.2 \cdot 10^{-2}$	24	$1.1 \cdot 10^{-2}$	40	$2.1 \cdot 10^{-5}$	56	$5.6 \cdot 10^{-12}$
9	$6.2 \cdot 10^{-2}$	25	$8.4 \cdot 10^{-3}$	41	$1.2 \cdot 10^{-5}$	57	$1.2 \cdot 10^{-12}$
10	$6.1 \cdot 10^{-2}$	26	$6.5 \cdot 10^{-3}$	42	$6.2 \cdot 10^{-6}$	58	$2.3 \cdot 10^{-13}$
11	$5.9 \cdot 10^{-2}$	27	$5 \cdot 10^{-3}$	43	$3.1 \cdot 10^{-6}$	59	$3.9 \cdot 10^{-14}$
12	$5.6 \cdot 10^{-2}$	28	$3.8 \cdot 10^{-3}$	44	$1.5 \cdot 10^{-6}$	60	$5.6 \cdot 10^{-15}$
13	$5.2 \cdot 10^{-2}$	29	$2.8 \cdot 10^{-3}$	45	$7.2 \cdot 10^{-7}$	61	$6.5 \cdot 10^{-16}$
14	$4.8 \cdot 10^{-2}$	30	$2 \cdot 10^{-3}$	46	$3.3 \cdot 10^{-7}$	62	$5.7 \cdot 10^{-17}$
15	$4.4 \cdot 10^{-2}$	31	$1.4 \cdot 10^{-3}$	47	$1.4 \cdot 10^{-7}$	63	$3.5 \cdot 10^{-18}$
16	$4 \cdot 10^{-2}$	32	$9.8 \cdot 10^{-4}$	48	$5.9 \cdot 10^{-8}$	64	$1.1 \cdot 10^{-19}$

$\mathbf{P}^{(e)}_{2\times16;1}$ (Figure 10a). Input of each $\mathbf{P}^{(e)}_{2\times16;1}$-box is divided into 16-bit left and 16-bit right inputs. The box $\mathbf{P}^{(e)}_{2\times16;1}$ is a set of 16 parallel $\mathbf{P}^{(e)}_{2;1}$-boxes controlled with the same bit e. The right (left) input (output) of 16 parallel boxes $\mathbf{P}^{(e)}_{2;1}$ compose the right (left) 16-bit input (output) of the box $\mathbf{P}^{(e)}_{2\times16;1}$. Thus, each of three boxes $\mathbf{P}^{(e)}_{2\times16;1}$ performs e-dependent swapping of the respective pair of the 16-bit components of the controlling vector V. For example, $\mathbf{P}^{(0)}_{2\times16;1}(V_1, V_6) = (V_1, V_6)$ and $\mathbf{P}^{(1)}_{2\times16;1}(V_1, V_6) = (V_6, V_1)$. Let the input vector of the box $\mathbf{P}^{(e)}_{96;1}$ be $(V_1, V_2, ...V_6)$. Then at the output of $\mathbf{P}^{(e)}_{96;1}$ we have $V' = (V_1, V_2, ..., V_6)$, if $e = 0$, or $V' = (V_6, V_5, ..., V_1)$, if $e = 1$. Structure of the switchable CP box $\mathbf{P}^{(V,e)}_{32;96}$ is shown in Figure 10b.

The switchable CP box $\mathbf{R}^{(V,e)}_{64;192}$ can be constructed with the use of transposition box $\mathbf{P}^{(e)}_{192;1}$ that is implemented as three parallel single-layer boxes $\mathbf{P}^{(e)}_{2\times32;1}$ (Figure 10c). Each $\mathbf{P}^{(e)}_{2\times32;1}$-box is a set of 32 parallel $\mathbf{P}^{(e)}_{2;1}$-boxes all of which are controlled with the bit e. The structure of the $\mathbf{R}^{(V,e)}_{64;192}$-box is shown in Figure 10d.

Use of the single-layer box to perform swapping components of the controlling vector V does not introduce essential additional time delay. Maximal introduced delay is $t_\oplus$ (time delay of the XOR operation). If V is set beforehand, then no additional delay is introduced.

Analogously to the construction of the $\mathbf{R}$-type COS boxes one can construct different variants of the the switchable COS boxes $\mathbf{S}^{(V,e)}_{32;96}$ and $\mathbf{S}^{(V,e)}_{64;192}$. For this purpose one can use the $\mathbf{S}_{2;1}$-involutions described, for example, by one of the following pairs of BFs[3] #17, #2, and #20 (see Table 2 and Figure 5).

In the design of switchable COS boxes for constructing the boxes $\mathbf{R}_{8;12}$ and $\mathbf{S}_{8;12}$,one can use also elementary boxes $\mathbf{R}_{2;1}$ and $\mathbf{S}_{2;1}$ that are not involutions. In this case the boxes $\mathbf{R}^{-1}_{8;12}$ and $\mathbf{S}^{-1}_{8;12}$ should be constructed using the respective inverses $\mathbf{R}^{-1}_{2;1}$ and $\mathbf{S}^{-1}_{2;1}$. Thus, we have large number of the potential variants of the switchable COS boxes appropriate to cryptographic applications. There are still more possibilities while designing switchable COS boxes combining different types of the $\mathbf{F}_{2;1}$-boxes. Below we shall consider the application of the switchable COS boxes in the design of the ciphers with simple key scheduling. The property of the controllability of the operations used as cryptographic primitives provides possibility to design different types of the iterative block cryptoschemes with simple key scheduling, which can be implemented in cheap hardware. The property of the switchability allows avoiding the weak keys while using the simple key scheduling.

4.2 Ciphers with Simple Key Scheduling

A number of the hardware-oriented DDP-based ciphers with simple key scheduling are presented in [5]. Using the respective COS boxes instead of the CP boxes in that ciphers one can reduce the number of rounds, however the problem of the weak keys, which is connected with the use of the simple key scheduling, remains unsolved. Below we represent ciphers SCOS-1, SCOS-2, and SCOS-3 as examples of the use of the switchable COS boxes in order to avoid weak keys and thwart slide attacks based on chosen structure of the key. If the simple key scheduling is used, then one can use equal subkeys and all encryption rounds will define the same substitution providing homogeneity of the encryption procedure, i.e. prerequisites for some successful slide attack [1, 2]. The switchable operation in the ciphers SCOS-1, SCOS-2, and SCOS-3 are used in a way preventing possibility to define homogeneity of the

Table 7: Distribution of the bits of the controlling data subblock

V_1	w_7	w_8	w_1	w_2	w_{16}	w_{15}	w_{10}	l_9	w_5	w_6	w_3	w_4	w_{11}	w_{12}	w_{13}	w_{14}
V_2	w_9	w_{10}	w_{11}	w_{12}	w_1	w_2	w_7	w_8	w_{13}	w_{14}	w_{15}	w_{16}	w_5	w_6	w_3	w_4
V_3	w_{13}	w_{14}	w_{15}	w_{16}	w_5	w_6	w_3	w_4	w_1	w_2	w_7	w_8	w_9	w_{10}	w_{11}	w_{12}
V_4	w_{21}	w_{22}	w_{29}	w_{30}	w_{25}	w_{26}	w_{23}	w_{24}	w_{31}	w_{32}	w_{27}	w_{28}	w_{17}	w_{18}	w_{19}	w_{20}
V_5	w_{31}	w_{32}	w_{27}	w_{28}	w_{17}	w_{18}	w_{19}	w_{20}	w_{29}	w_{30}	w_{25}	w_{26}	w_{21}	w_{22}	w_{23}	w_{24}
V_6	w_{19}	w_{20}	w_{23}	w_{24}	w_{27}	w_{28}	w_{29}	w_{30}	w_{21}	w_{22}	w_{17}	w_{18}	w_{32}	w_{31}	w_{25}	w_{26}

encryption procedure by choosing certain types of keys.

Figure 11 presents round encryption function of SCOS-1. The 32-bit round subkeys are denoted as K_r, G_r, and T_r. Two input data subblocks A and B are of the 32-bit length. The operational boxes $\mathbf{S}^{(e)}_{32;96}$, $\mathbf{R}^{(e)}_{32;96}$, and $\mathbf{P}^{(e)}_{2\times32;1}$ have been specified in Section 4.1. The extension box $\mathbf{E}$ used to form the controlling vector of the corresponding operations is described by Table 7, where bits w_i correspond to vector $W = (w_1, w_2, ..., w_{32})$ that is input of the $\mathbf{E}$-box and the output vector is $V = (V_1, V_2, ..., V_6)$. For example, in line with Table 7 we have $V_1 = (w_7, w_8, w_1, w_2, w_{16}, w_{15}, w_{10}, w_9, w_5, w_6, w_3, w_4,$ w_{11}, w_{12}, w_{13}, $w_{14})$. The extension box $\mathbf{E}$ has been constructed in accordance with the following criteria:

1) *Let X be the input n-bit vector of one of the boxes $\mathbf{R}^{(e)}_{32;96}$ and $\mathbf{S}^{(e)}_{32;96}$. Then for all W and i the bit x_i should be permuted depending on six different bits of W.*

2) *For all i the bit w_i should define exactly three bits of V.*

The first criterion provides that each output of the switchable COS box is some BF in $\mu = 63$ variables, where 32 variables are the bits of the current transformed data subblock and 31 variables are 31 bits of the current controlling data subblock. The second-type extension box $\mathbf{E}'$ used in SCOS-1 is specified as follows: $\mathbf{E}'(W) = \mathbf{E}(W^{>>>16})$. The box $\mathbf{E}'$ also satisfies criteria 1 and 2.

The generalized encryption procedure is the following one:

1) Perform initial transformation: $A := A \oplus G_0$ and $B := B \oplus T_0$.

2) For rounds $r = 1$ to 8 do {Perform the round transformation and swap data subblocks}.

3) Swap data subblocks and perform final transformation: $A := A \oplus G_9$ and $B := B \oplus T_9$.

The cipher SCOS-1 uses the 128-bit key $Q = (Q_1, Q_2, Q_3, Q_4)$ represented as concatenation of four 32-bit keys. The key scheduling and specification of the switching bits are presented in Table 8. The cipher SCOS-1 is oriented to cheap hardware implementation. An interesting peculiarity of this cryptoscheme is the high parallelism of the computations. Indeed, the operations $\mathbf{S}^{(e_1)}_{32;96}$ and $\mathbf{R}^{(e_2)}_{32;96}$ are performed in parallel and then the operations $\mathbf{S}^{(e_3)}_{32;96}$ and $\mathbf{R}^{(e_4)}_{32;96}$ are performed also in parallel.

The COS-box operations can be easily embedded in microcontrollers and general purpose CPUs and used while designing fast firmware and software encryption systems. Figure 12 shows round functions of the firmware-suitable COS-based ciphers SCOS-2 (a) and SCOS-3 (b) working with the 128-bit key $Q = (Q_1, Q_2, Q_3, Q_4)$. The generalized encryption scheme of the both ciphers is presented in Figure 12(c). The final transformation in SCOS-2 is performed as swapping subblocks and performing two XOR operations: $A := A \oplus G_{13}$ and $B := B \oplus T_{13}$. In SCOS-3 the final transformation is performed as follows: $A := A -_{32} G_{13}$ and $B := B +_{32} T_{13}$. Table 9 presents the key scheduling and specification of the switching bits for SCOS-2 and SCOS-3 (both ciphers use the identical key scheduling for $e = 0$).

4.3 Estimate of the Hardware Implementation and Security

While the FPGA implementation of the cipher SCOS-1 oriented to hardware the consumption of the logical cells is independent of type of the boxes $\mathbf{R}_{2;1}$ and $\mathbf{S}_{2;1}$ used as elementary building blocks for constructing the boxes $\mathbf{R}^{(e)}_{32;96}$ and $\mathbf{S}^{(e)}_{32;96}$. While the VLSI implementation the critical path and required number of nand-gates depend on the type of the elementary building blocks, however in all cases the implementation cost and the depth of the critical path are comparatively small.

The time delay corresponding to one active layer of the boxes $\mathbf{R}^{(e)}_{32;96}$ and $\mathbf{S}^{(e)}_{32;96}$ equals from $t_\oplus$ to $2t_\oplus$, where $t_\oplus$ is the time delay of the XOR operation. Time delay of the switchable operational boxes used in the described ciphers can be estimated as from $6t_\oplus$ to $12t_\oplus$ (we consider six-layer COS boxes). The critical path of one round of the cipher SCOS-1 equals from $15t_\oplus$ to $27t_\oplus$. The critical path of eight rounds of SCOS-1 equals from $122t_\oplus$ to $218t_\oplus$ (see Table 11).

Conservative estimate shows that implementation of the boxes $\mathbf{R}^{(e)}_{32;96}$ and $\mathbf{S}^{(e)}_{32;96}$ takes about from 800 to 1000 nand-gates. The last figures define the implementation cost of the additional instruction of some hypothetical microcontroller while implementing the ciphers SCOS-2 and SCOS-3 in firmware.

One round of the hardware-oriented ciphers SCOS-

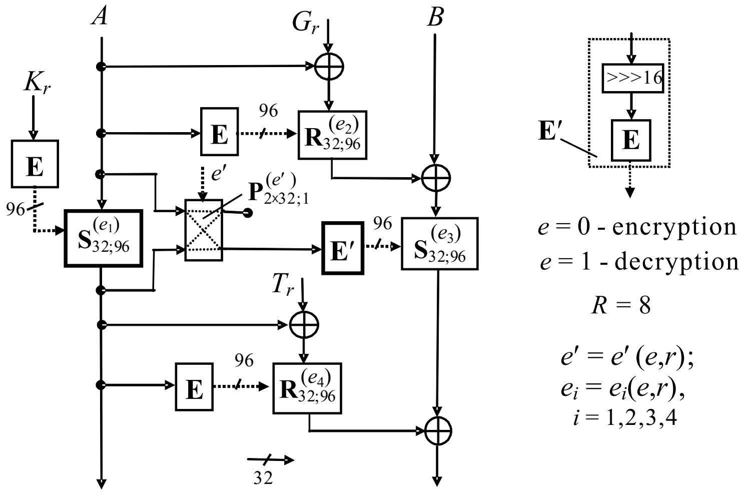
A
G_r
B
K_r
E
96
E
96
$\mathbf{R}_{32;96}^{(e_2)}$
E′
>>>16
E
e'
$\mathbf{P}_{2\times32;1}^{(e')}$
96
$\mathbf{S}_{32;96}^{(e_1)}$
E′
96
$\mathbf{S}_{32;96}^{(e_3)}$
$e = 0$ - encryption
$e = 1$ - decryption
T_r
$R = 8$
96
E
$\mathbf{R}_{32;96}^{(e_4)}$
$e' = e'(e,r)$;
$e_i = e_i(e,r)$,
$i = 1,2,3,4$
32

Figure 11: Encryption round in SCOS-1

Table 8: SCOS-1: specification of the switching bits and round subkeys

Round	$e=0$			$e=1$			$e=0$					$e=1$				
r	K_r	G_r	T_r	K_r	G_r	T_r	e_1	e_2	e_3	e_4	e'	e_1	e_2	e_3	e_4	e'
0	-	Q_2	Q_1	-	Q_1	Q_4	-	-	-	-	-	-	-	-	-	-
1	Q_1	Q_2	Q_3	Q_1	Q_3	Q_2	1	0	1	0	0	0	0	1	1	0
2	Q_4	Q_1	Q_2	Q_2	Q_4	Q_1	0	1	1	1	1	1	1	1	1	0
3	Q_3	Q_4	Q_1	Q_4	Q_1	Q_3	0	0	0	0	0	0	0	1	0	1
4	Q_2	Q_3	Q_4	Q_3	Q_2	Q_1	1	0	1	1	0	0	0	0	1	0
5	Q_3	Q_1	Q_2	Q_2	Q_4	Q_3	1	1	1	0	1	0	1	0	0	1
6	Q_4	Q_3	Q_1	Q_3	Q_1	Q_4	1	0	0	0	0	1	0	1	0	1
7	Q_2	Q_1	Q_4	Q_4	Q_2	Q_1	0	1	0	1	1	1	1	0	1	0
8	Q_1	Q_2	Q_3	Q_1	Q_3	Q_2	1	1	0	0	1	0	0	0	0	1
9	-	Q_1	Q_4	-	Q_2	Q_1	-	-	-	-	-	-	-	-	-	-

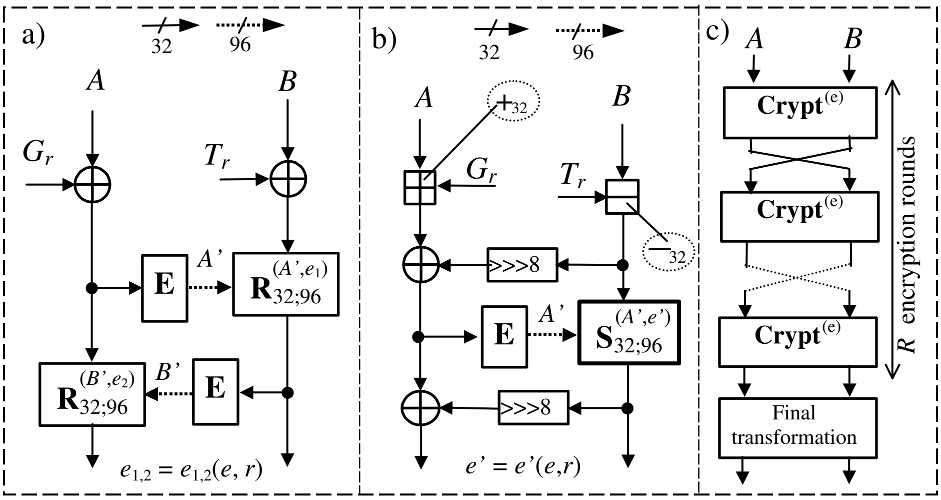

Figure 12: The firmware-suitable ciphers: a – SCOS-2, b – SCOS-3, c – general structure of transformation procedure

Table 9: SCOS-2 and SCOS-3: Specification of the switching bits and round subkeys (final transformation is denoted as $r = 13$)

r	$e = 0$		$e = 1$		$e = 1$		$e = 0$			$e = 1$		
	SCOS-2(3)		SCOS-2		SCOS-3							
	G_r	T_r	G_r	T_r	G_r	T_r	e_1	e_2	e'	e_1	e_2	e'
1	Q_1	Q_2	Q_2	Q_3	Q_2	Q_3	1	0	1	0	1	1
2	Q_3	Q_4	Q_1	Q_4	Q_4	Q_1	0	0	0	1	0	0
3	Q_3	Q_2	Q_3	Q_2	Q_2	Q_3	1	1	1	0	0	0
4	Q_4	Q_1	Q_4	Q_1	Q_1	Q_4	0	1	0	1	0	1
5	Q_4	Q_3	Q_3	Q_1	Q_1	Q_3	1	0	1	1	1	0
6	Q_1	Q_2	Q_4	Q_2	Q_2	Q_4	1	1	1	0	1	0
7	Q_4	Q_3	Q_4	Q_3	Q_3	Q_4	0	1	0	0	0	0
8	Q_4	Q_2	Q_1	Q_2	Q_2	Q_1	0	0	0	1	0	0
9	Q_3	Q_1	Q_4	Q_3	Q_3	Q_4	1	0	1	0	1	1
10	Q_4	Q_1	Q_4	Q_1	Q_1	Q_4	1	1	1	0	0	0
11	Q_3	Q_2	Q_3	Q_2	Q_2	Q_3	1	0	1	1	1	1
12	Q_1	Q_4	Q_3	Q_4	Q_4	Q_3	0	1	0	1	0	0
13	Q_2	Q_3	Q_1	Q_2	Q_1	Q_2	-	-	-	-	-	-

1 can be implemented using about from 3,600 to 4,400 gates, respectively. In the case of the implementation hardware architecture described in [7] all rounds of the ciphers are implemented. For full round ciphers we have the implementation cost from 28,800 to 35,200 nand-gates. To the last figures one should add some gate count corresponding to the key scheduling, 128-bit register for key and to two 64-bit registers for input and output data. This makes about 1,500 additional nand-gates. The whole implementation cost of SCOS-1 is presented in Table 11 which presents hardware evaluation comparing different ciphers (figures marked with * relates to [7]).

One can see that the fastest implementation corresponds to 128-bit cipher Rijndael (performance $z \approx 1.35$ bit/$t_\oplus$) and the cheapest one corresponds to SCOS-1 (470…580 gate/bit). The SCOS-1 ($z \approx 0.30 \ldots 0.53$ bit/$t_\oplus$) is faster than RC6 ($z \approx 0.15$ bit/$t_\oplus$), Triple-DES ($z \approx 0.29$ bit/$t_\oplus$), and Twofish ($z \approx 0.27$ bit/$t_\oplus$). It is remarkable that SCOS-1 is cheaper than DES (≈ 840 gate/bit).Hardware implementation efficacy of the SCOS-1 is explained by designing it at bit level.

Our preliminary security estimations for SCOS-1, SCOS-2, and SCOS-3 show that all of them are indistinguishable from a random cipher with differential, linear and other attacks. The most useful linear and differential characteristics (DCs) correspond to the case of few active bits, the differential attack (DA) being more efficient than linear one. The last corresponds to the results on analysis of different DDP-based ciphers presented in [5]. Results of our rough security estimation against DA are presented in Table 10, where R is the full number of encryption rounds and $p(r) = \Pr\left(\Delta \xrightarrow{r} \Delta'\right)$ is the probability that the Δ input difference transforms into the Δ' output difference when passing through r rounds.

For the considered ciphers the most efficient is the two-round iterative DC with the difference (Δ_0^A, Δ_1^B), where indices indicates the number of active bits. Its contribution to the to probability $p(R) = \Pr\left((\Delta_0^A, \Delta_1^B) \xrightarrow{R} (\Delta_0^A, \Delta_1^B)'\right)$ is less than 2^{-78}. Note that Δ_1^B denotes arbitrary difference with one active bit in the right data subblock, i.e. Δ_1^B denotes a batch of the one bit differences. The results of the DA security estimate of the described above ciphers show that they are indistinguishable from a random cipher with DA using the considered iterative DC (see Table 10). Presented ciphers are only the illustrations of the design peculiarities connected with the use of the COS box operations.

Table 10: Contribution of the two-round DC to the probability $p(R) = \Pr\left((\Delta_0^A, \Delta_1^B) \xrightarrow{R} (\Delta_0^A, \Delta_1^B)'\right)$

Cipher	R	Difference	$p(2)$	$p(R)$
SCOS-1	8	(Δ_0^A, Δ_1^B)	$< 2^{-28}$	$< 2^{-112}$
SCOS-2	12	(Δ_0^A, Δ_1^B)	$< 2^{-16}$	$< 2^{-96}$
SCOS-3	12	(Δ_0^A, Δ_1^B)	$< 2^{-13}$	$< 2^{-78}$

5 Conclusion

This research has shown that previously proposed DDPs are only a particular representatives of the wide class of DDO performed with the COS boxes. Furthermore, there exist many different types of the elementary building blocks $\mathbf{F}_{2;1}$ providing construction of the COS boxes that are more attractive as cryptographic primitive than the CP boxes. Using variety of the proposed DDP-based cryptoschemes [5, 11] and replacing the CP boxes by

Table 11: Hardware evaluation of SCOS-1 against some well-known ciphers

Cipher	Gate count		Critical path, $t_{\oplus}$	
	key schedule	encryption	key setup,	encryption
SCOS-1	500	29,800... ...36,200	-	122 210
DES	12,000*	42,000*	-	80
Triple-DES	23,000*	120,000*	-	220
Rijndael	94,000*	520,000*	83	95
RC6	900,000*	740,000*	3000	880
Twofish	230,000*	200,000*	23	470

the corresponding COS boxes one can construct different block ciphers that allows one to obtain the required avalanche, correlation-immunity, and propagation properties with fewer number of rounds. This leads to decrease of the hardware implementation cost and to the performance increase. However, in certain applications the CP boxes are preferable, for example, in the case of implementing a new CPU instruction suitable to perform some DDO [5]. Different types of new controlled operations can be constructed (1) using the fixed topology and different types of the boxes $\mathbf{F}_{2;1}$, (2) using the fixed type of the elementary COS boxes and different topologies, and (3) mixing different types of the COS boxes in different used topologies.

We have proposed some specific topologies of the COS boxes and several COS-based block ciphers, however they are presumably only implementation examples. Using methodology [5] of the block cipher design based on the use of the controlled operations the reader can easy construct many other cryptosystems having high security against known attacks. While using the key preprocessing one can efficiently apply the COS boxes in order to construct strong key scheduling oriented to minimizing the consumption of the additional hardware resources. The COS boxes are also very interesting for the use in the hash function design.

While using the simple key scheduling in the block cipher design one can apply the switchable COS boxes that should provide (1) avoiding the weak keys and (2) security against slide attacks based on chosen key. However, justification of such approach to the design of the ciphers with simple key scheduling require further investigation regarding different other security aspects. Our results give only the initial bar to undertake further research in this direction.

Thus, this paper introduces a class of new controlled primitives enriching the DDO-based design of fast ciphers and diversifies the class of the switchable controlled operations.

References

[1] A. Biryukov and D. Wagner, "Slide attacks," in *Proceedings of the 6th International Workshop, Fast Software Encryption - FSE '99*, LNCS 1636, pp. 245-259, Springer-Verlag, 1999.

[2] A. Biryukov and D. Wagner, "Advanced slide attacks," in *Advances in Cryptology - Eurocrypt'2000*, LNCS 1807, pp. 589-606, Springer-Verlag, 2000.

[3] C. Burwick, D. Coppersmith, E. D'Avingnon, R. Gennaro, Sh. Halevi, Ch. Jutla, Jr. S. M. Matyas, L. O'Connor, M. Peyravian, D. Safford, and N. Zunic, "MARS - a candidate cipher for AES," in *1st Advanced Encryption Standard Candidate Conference Proceedings*, Venture, California, Aug. 20-22, 1998.

[4] C. Clos, "A study of nonblocking switching networks," *Bell System Technical J.*, vol. 32, pp.406-424, 1953.

[5] N. D. Goots, B. V. Izotov, A. A. Moldovyan, and N. A. Moldovyan, *Modern cryptography: protect your data with fast block ciphers*, Wayne, A-LIST Publishing, 2003. (www.alistpublishing.com).

[6] N. D. Goots, A. A. Moldovyan, and N. A. Moldovyan, "Fast encryption algorithm SPECTR-H64," in *Proceedings of the International Workshop, Methods, Models, and Architectures for Network Security*, LNCS 2052, pp. 275-286, Springer-Verlag, 2001.

[7] T. Ichikawa, T. Kasuya, and M. Matsui, "Hardware evaluation of the AES finalists," in *3rd Advanced Encryption Standard Conference Proceedings*, New York, NY, USA, Apr. 13-14, 2000. (http://www.nist.gov/aes)

[8] Y. Ko, D. Hong, S. Hong, S. Lee, and J. Lim, "Linear cryptanalysis on SPECTR-H64 with higher order differential property," in *Proceedings of the 2nd International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security - MMM-ACNS 2003*, LNCS 2776, pp. 298-307, Springer-Verlag, 2003.

[9] M. Kwan, "The design of the ICE encryption algorithm," in *Proceedings of the 4th International Workshop, Fast Software Encryption - FSE '97*, LNCS 1267, pp. 69-82, Springer-Verlag, 1997.

[10] V. M. Maslovsky, A. A. Moldovyan, and N. A. Moldovyan, *A method of the block encryption of discrete data*, Russian patent # 2140710, Bull. no 30, 1999.

[11] A. A. Moldovyan and N. A. Moldovyan, "OA cipher based on data-dependent permutations," *Journal of Cryptology*, vol. 15, no. 1, pp. 61-72, 2002.

[12] D. S. Parker, "Notes on shuffle/exchange-type switching networks," *IEEE Transactions on computers*, vol. C-29, no. 3, pp. 213-222, 1980.

[13] M. Portz, "A generallized description of DES-based and Benes-based permutation generators," LNCS 718, pp. 397-409, Springer-Verlag, 1992.

[14] R. L. Rivest, "The RC5 encryption algorithm," in *Proceedings of the 2nd International Workshop, Fast Software Encryption - FSE'94*, LNCS 1008, pp. 86-96, Springer-Verlag, 1995.

[15] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, 'The RC6 block cipher," in *1st Advanced Encryption Standard Candidate Conference Proceedings*, Venture, California, Aug. 20-22, 1998.

[16] B. Van Rompay, L. R. Knudsen, and V. Rijmen, "Differential cryptanalysis of the ICE encryption algorithm," in *Proceedings of the 6th International Workshop, Fast Software Encryption - FSE'98*, LNCS 1372, pp. 270-283, Springer-Verlag, 1998.

[17] N. Sklavos, N. A. Moldovyan, and O. Koufopavlou, "High speed networking security: design and implementation of two new DDP-based ciphers," *Mobile Networks and Applications, Special Issue on : Algorithmic Solutions for Wireless, Mobile, Ad Hoc and Sensor Networks, MONET Journal,* Kluwer, (in print), 2004..

[18] J. Seberry, X-M. Zhang, and Y. Zheng, "Nonlinearly balanced Boolean functions and their propagation characteristics," in *Advances in cryptology - CRYPTO'93*, LNCS 773, pp. 49-60, Springer-Verlag, 1994.

[19] A. A. Waksman, "Permutation network," *Journal of the ACM*, vol. 15, no. 1, pp. 159-163, 1968.

Nikolay A. Moldovyan is an honored inventor of Russian Federation (2002), a chief researcher with the Specialized Center of Program Systems "SPECTR", and a Professor with the Saint Petersburg Electrical Engineering University. His research interests include computer security and cryptography. He has authored or co-authored more than 50 patents and 200 scientific articles, books, and reports. He received his Ph.D. from the Academy of Sciences of Moldova (1981). Contact him at: nmold@cobra.ru.

Alexander A. Moldovyan is a chief constructor with the Specialized Center of Program Systems "SPECTR", and a Professor with the State University For Waterway Communications (Saint Petersburg, Russia). His research interests include information assurance, computer security and applied cryptography. He has authored or co-authored more than 35 patents and 150 scientific articles, books, and reports. He received his Ph.D. from the Saint Petersburg Electrical Engineering University (1996). Contact him at: ma@cobra.ru.

Michael A. Eremeev is a Professor with the Military Engineering-Space Academy (Saint Petersburg, Russia). His research interests include cryptography, communication and network security. He has authored or co-authored 3 patents and more than 90 scientific articles, books, and reports. He received his Ph.D. from the Military Engineering-Space Academy (1996). Contact him at: nmold@cobra.ru.