New Class of Cryptographic Primitives and Cipher Design for Networks Security

Nikolay A. Moldovyan[1], Alexander A. Moldovyan[1], Michael A. Eremeev[1], and Nicolas Sklavos[2]
(Corresponding author: Nikolay A. Moldovyan)

Specialized Center of Program Systems, SPECTR[1]
Kantemirovskaya Str. 10, St. Petersburg 197342, Russia (Email: nmold@cobra.ru)
Electrical & Computer Engineering Department, University of Patras,[2]
Greece (Email: nsklavos@ieee.org)

(Received July 15, 2005; revised and accepted Aug. 10, 2005)

Abstract

This work focuses the problem of increasing the integral implementation efficacy of block ciphers. It proposes a new approach to the cipher design, suitable to applications, where constrained resources are available to embedded security mechanisms, such as ad-hoc, sensor and wireless networks. The paper develops the cipher design approach based on the use of data-dependent (DD) operations (DDOs). A new class of DDO based on the advanced controlled elements (CEs) is introduced, which is proven well suited to hardware implementations, for ASIC and FPGA devices. Classification of the CEs and properties of some new DDOs are also presented. A new DDO-based cipher design is considered, which is more efficient for VLSI implementation than AES finalists and other known DDO-based ciphers. For the proposed cipher, Eagle-128, both ASIC and FPGA implementation results are presented. Finally comparisons with other published implementations are illustrated, using the Performance/Cost ratio and Performance/(Cost*Frequency) ratio indices.

Keywords: Block ciphers, data dependent operations, networks security, VLSI implementation

1 Introduction

Security is an issue that has attracted the research community interest the last years, especially in the field of ad-hoc and sensor networks. The communication revolution has triggered the high needs for encryption algorithms and security schemes. The data-dependent (DD) permutations (DDP) have been proved as an efficient cryptographic primitive for the design of the hardware-oriented ciphers [6, 10]. The DDP are performed with so called controlled permutation (CP) boxes $\mathrm{P}_{n/m}$ with n-bit input, n-bit output, and m-bit control input. A CP box is implemented as some controlled permutation network having the layered topology (Figure 1). The standard building block of the CP boxes is the switching element $\mathbf{P}_{2/1}$ (Figure 1b) representing some elementary CP box controlled by one bit $v : y_1 = x_{1+v}$ and $y_2 = x_{2-v}$. In the schematics the solid lines indicate data movement, while dotted lines indicate the controlling bits. Depending on the controlling vector V, a CP box performs bit permutation, called modification of the CP-box operation and denoted as $\mathrm{P}^{(V)}_{n/m}$.

The CP boxes can be considered as a particular case of the controlled substitution permutation networks (CSPNs), built up using the minimum size controlled elements (CEs) $\mathbf{F}_{2/1}$. In general case, a CE $\mathbf{F}_{2/1}$ (Figure 2a) represents a switchable 2×2 substitution box. It implements (Figure 2b) two different linear substitutions S_1 (if the controlling bit $v = 0$) and S_2 (if $v = 1$); performed on a two-bit vector (x_1, x_2). Analogously to CP boxes different types of the CSPNs constructed using CEs $\mathbf{F}_{2/1}$ can be applied as DDOs that are suitable to designing fast hardware-oriented ciphers. For FPGA implementation, that has gained highly significant practical importance, all types of the CEs $\mathbf{F}_{2/1}$ are implemented using two 4-bit memory cells (Figure 2c). Each cell implements a Boolean Function (BF) in three variables. A step to advance the DDO-based cipher design, is to select and use non-linear CEs $\mathbf{F}_{2/1}$ with maximum non-linearity [5], instead of the switching elements $\mathbf{P}_{2/1}$ that are linear cryptographic primitives.

It has been estimated that the implementation of the $\mathbf{F}_{2/1}$ elements needs only 50% of the resources of two standard cells of a typical FPGA device and there exist some prerequisites to implement some advanced CEs.

In this paper, another approach to increase the efficiency of the FPGA implementation of the DDO-based ciphers is introduced. The $\mathbf{F}_{2/2}$ type CEs controlled with two bits v and z (Figure 3a) are proposed as main building block, while designing the DDO boxes. An element $\mathbf{F}_{2/2}$

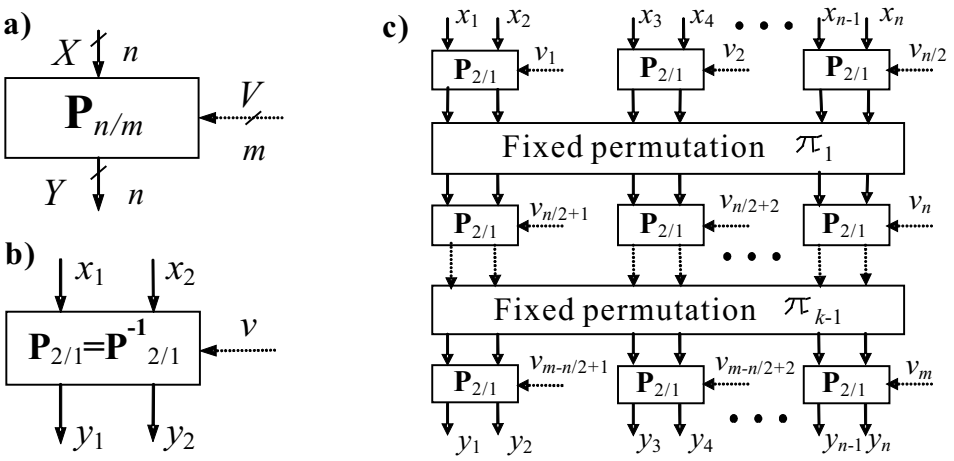


Figure 1: Notation of (a) the $\mathbf{P}_{n/m}$-box, (b) $\mathbf{P}_{2/1}$-box, (c) input bits x_1 and x_4 should be indicated; in two boxes in the left-upper corner should be written "$\mathbf{P}_{2/1}$")

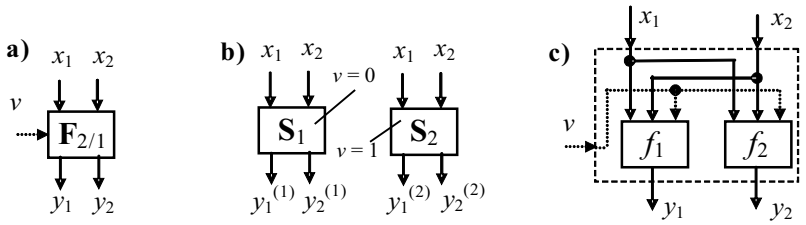


Figure 2: Element $\mathbf{F}_{2/1}$ (a) represented as switchable 2×2 substitution (b) or as a pair of BFs in three variables (c)

can be described as a pair of BFs with four variables (Figure 3b), or as a set of four 2×2 substitutions (Figure 3c) called modifications $\mathbf{F}_{2/2}^{(00)}$, $\mathbf{F}_{2/2}^{(01)}$, $\mathbf{F}_{2/2}^{(10)}$ and $\mathbf{F}_{2/2}^{(11)}$. The VLSI implementation of the $\mathbf{F}_{2/2}$ element needs also two 4-bit memory cells. Elements $\mathbf{F}_{2/2}$ realize transformation of the two-bit input vectors (x_1, x_2), which is described by BF having larger non-linearity value NL (non-linearity in the sense of the distance of non-linear BF from the set of affine BFs in the same number of variables). They also have higher degree of algebraic normal form than BF corresponding to transformation defined by CEs $\mathbf{F}_{2/1}$. Therefore CEs $\mathbf{F}_{2/2}$ are proven to be more powerful cryptographic primitives. They potentially support designing more efficient CEs than elements $\mathbf{F}_{2/1}$. With the applied advanced DDOs the design of ciphers with less number of rounds is supported, yielding to higher Performance/Cost ratio.

The rest of the paper is organized as follows: Section 2 introduces the criteria to select CEs $\mathbf{F}_{2/2}$ and presents classification of the $\mathbf{F}_{2/2}$ CEs that are involutions. The topology of DDO boxes is also described in the same section. In Section 3 a new DDO-based cipher, is proposed, well suited to VLSI implementations. In Section 4, both ASIC and FPGA implementations synthesis results are presented. Comparisons with other known ciphers are also given. Finally, in Section 5 conclusions and outlook are discussed.

2 New Class of DDO Boxes

2.1 Criteria and Classification

In order to select the $\mathbf{F}_{2/2}$ CEs suitable to design efficient cryptographic DDOs, the following criteria have to be applied:

- Criterion C1: *Each one of the two outputs of CEs should be a non-linear BF having maximum possible non-linearity NL = 4 for balanced BFs in four variables.*
- Criterion C2: *Each modification of CEs should be bijective transformation* $(x_1, x_2) \rightarrow (y_1, y_2)$.
- Criterion C3: *Each modification of CEs should be involution.*
- Criterion C4: *The linear combination of two outputs of CEs, i.e.* $f_3 = y_1 \oplus y_2$, *should have maximum possible non-linearity NL = 4 for balanced BFs in four variables..*

Different DDOs can be implemented replacing the switching elements in the known DDP boxes by the $\mathbf{F}_{2/2}$ CEs. Due to Criterion C3 such replacement in two mutual inverse DDP boxes yields two mutual inverse DDOs for the same FPGA device resources being used. The

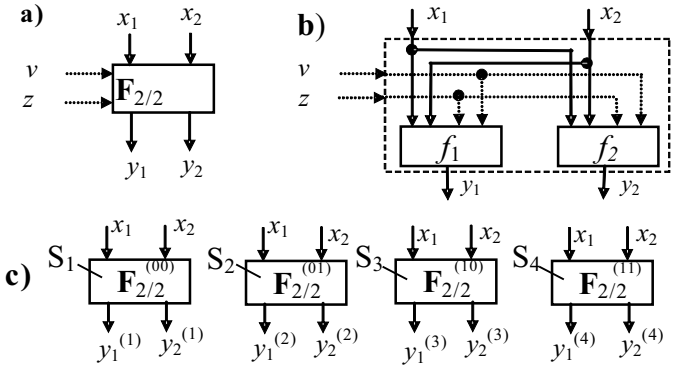


Figure 3: Element $\mathbf{F}_{2/2}$ (a) represented as a pair of BFs in four variables (b) or as four 2×2 substitutions (c)

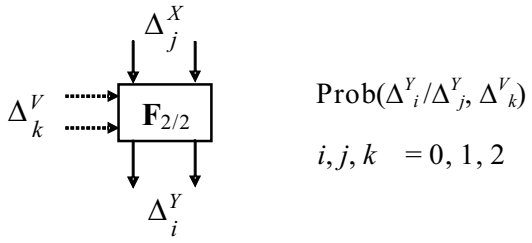


Figure 4: Differential characteristics of the $\mathbf{F}_{2/2}$ elements

Table 1: Examples of DCs of the $\mathbf{F}_{2/2}$ elements

i	j	k	A	B	C	D	E
0	1	0	0	0	0	0	0
1	1	0	3/4	5/8	7/8	1/2	1
2	1	0	1/4	3/8	1/8	1/2	0
0	2	0	0	0	0	0	0
1	2	0	1/2	3/4	1/4	1	0
2	2	0	1/2	1/4	3/4	0	1

switching element $\mathbf{P}_{2/1}$, (that is proven as efficient minimum size cryptographic primitive for designing variable operations, the $\mathbf{P}_{2/1}$ CE is a linear elementary operation though) satisfies only Criteria C1-C3. The Criterion C4 defines selection of the advanced CEs that are non-linear primitives. In order to try all possible variants of the $\mathbf{F}_{2/2}$ elements we have considered the $\mathbf{F}_{2/2}$ elements as sets of four 2×2 substitutions (S_1, S_2, S_3, S_4). Each substitution is one of involutions shown in Figure 5 (which is sufficient due to Criterion C3). For some CE $\mathbf{F}_{2/2}$ defined as a set (S_1, S_2, S_3, S_4) we can easy get BFs describing its outputs y_1 and y_2 (Figure 2):

$$y_1 = vz(y_1^{(1)} \oplus y_1^{(2)} \oplus y_1^{(3)} \oplus y_1^{(4)}) \oplus v(y_1^{(1)} \oplus y_1^{(3)}) \oplus z(y_1^{(1)} \oplus y_1^{(2)}) \oplus y_1^{(1)}$$

$$y_2 = vz(y_2^{(1)} \oplus y_2^{(2)} \oplus y_2^{(3)} \oplus y_2^{(4)}) \oplus v(y_2^{(1)} \oplus y_2^{(3)}) \oplus z(y_2^{(1)} \oplus y_2^{(2)}) \oplus y_2^{(1)}.$$

For example, for the (h, f, e, j) element we have:

$$y_1 = vzx_2 \oplus vz \oplus vx_1 \oplus zx_1 \oplus z \oplus x_1 \oplus x_2 \qquad NL(y_1) = 4$$

$$y_2 = vzx_1 \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus zx_2 \oplus z \oplus x_2 \qquad NL(y_2) = 4$$

$$y_1 \oplus y_2 = vzx_1 \oplus vzx_2 \oplus vz \oplus vx_2 \oplus zx_2 \oplus x_1 \qquad NL(y_1 \oplus y_2) = 4.$$

While performing DDOs some bits of data are used as v, z, x_1, x_2, therefore we have non-linear transformation performed on some encrypted data block. We have established that there exist 2208 CEs $\mathbf{F}_{2/2}$ satisfying the Criteria 1-4.

Besides the NL value and the algebraic degree of BF, differential characteristics (DCs) of the CE are important to characterize CEs as cryptographic primitives. We have studied full set of the DCs, for all elements $\mathbf{F}_{2/2}$. Possible DCs are illustrated in Figure 4, where $p(\Delta_i^Y/\Delta_j^X, \Delta_k^V)$ is probability to have the output difference Δ_i^Y, if the input difference is Δ_j^X and the difference at the controlling input is Δ_k^V (indices indicate the number of non-zero bits in corresponding differences). For the case k = 0 we have found that there exist only five types (A, B, C, D, and E) of DCs corresponding to the non-linear $\mathbf{F}_{2/2}$ CEs. Among 2208 CEs $\mathbf{F}_{2/2}$ having maximum non-linearity ($NL(f_1) = NL(f_2) = NL(f_1) = 4$) we have got four different types of DCs: A, B, D, and E. The results are presented in the following Table 1.

To characterize all DCs we introduce the integral parameter called average entropy defined as follows:

$$\overline{\mathrm{H}} = \frac{(\sum_{j=0}^{2}\sum_{k=1}^{2}\mathrm{H}_{jk} + \sum_{j=1}^{2}\mathrm{H}_{j0})}{8},$$

where $\mathrm{H}_{jk} = -\sum_{i=0}^{2} p(\Delta_i^Y/\Delta_j^X,\ \Delta_k^V)\log_3 p(\Delta_i^Y/\Delta_j^X,\ \Delta_k^V)$. Table 2 presents classification of the $\mathbf{F}_{2/2}$ elements having maximum non-linearity.

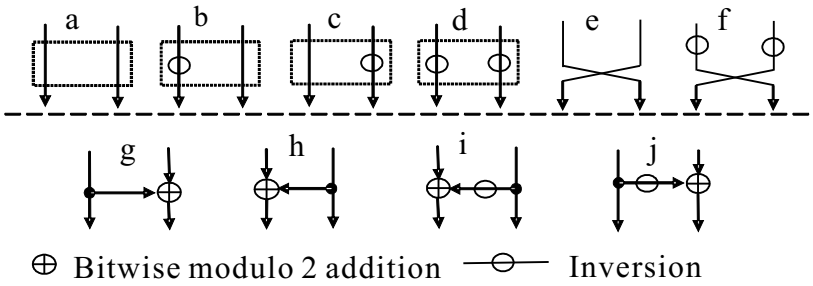


Figure 5: All existing 2×2 substitutions that are involutions

Thus, due to non-linearity and better DCs the $\mathbf{F}_{2/2}$ elements are significantly more attractive as cryptographic primitives than $\mathbf{P}_{2/1}$ and $\mathbf{F}_{2/1}$.

2.2 Controlled Operational Boxes

Let us consider an active cascade in some CSPN constructed using CEs $\mathbf{F}_{2/2}$ (Figure 6a). The controlling vector corresponding to the active cascade can be denoted as (V_j, Z_j), where j is the number of the cascade, $V_j, Z_j \in \{0,1\}^{n/2}$, and n is the input size of the CSPN. The full controlling vector of the CSPN with s cascades is denoted as follows: $(V, Z) = (V_1, Z_1, V_2, Z_2, \cdots, V_s, Z_s)$. In order to construct a DDO boxes $\mathbf{F}_{64/384}$ and $\mathbf{F}^{-1}_{64/384}$ with 64-bit input we use mutually inverse boxes $\mathbf{F}_{8/24}$ and $\mathbf{F}^{-1}_{8/24}$ (see Figure 6b and 6c). Analogously to construction of the mutual inverse DDP boxes [6] in the $\mathbf{F}_{64/384}$ ($\mathbf{F}^{-1}_{64/384}$) box the active cascades are numbered from top (bottom) to bottom (top).

The boxes $\mathbf{F}_{64/384}$ and $\mathbf{F}^{-1}_{64/384}$ can be represented as the superposition $\mathbf{F}_{64/192} \bullet \mathbf{I}_1 \bullet \mathbf{F}^{-1}_{64/192}$ in which the boxes $\mathbf{F}_{64/192}$ and $\mathbf{F}^{-1}_{64/192}$ are controlled with independent binary vectors. The permutational involution $\mathbf{I}_1$ is described as follows:

$$(1)(2,9)(3.17)(4,25)(5,33)(6,41)(7,49)(8,57)(10)$$
$$(11,18)(12,26)(13,34)(14,42)(15,50)(16,58)(19)$$
$$(20,27)(21,35)(22,43)(23,51)(24,59)(28)(29,36)$$
$$(30,44)(31,52)(32,60)(37)(38,45)(39,53)(40,61)$$
$$(46)(47,54)(48,62)(55)(56,63)(64).$$

Differential properties of the boxes $\mathbf{F}_{64/384}$ and $\mathbf{F}^{-1}_{64/384}$ depend on the type of the $\mathbf{F}_{2/2}$ element used as standard building block, i. e. on its DCs. To compare avalanche introduced by different types of the $\mathbf{F}_{64/384}$ boxes, we have considered the probability to have at the output the difference with the weight $wt(\Delta y)$, provided the input difference has the weight $wt(\Delta x) = 1$. This probability is denoted as :

$$p\{wt(\Delta y)/wt(\Delta x) = 1, wt(\Delta v, \Delta z) = 0\}$$

Using the method of generating functions and data from Table 1, one can easily calculate the probability for different values $wt(\Delta y)$. For the $\mathbf{F}_{2/2}$ elements of the types A, B, C, D, and E we have the following generating functions:

$$A: \quad \varphi_2^{\mathbf{F_{2/2}}}(z) = \frac{3}{4}z + \frac{1}{4}z^2;$$
$$B: \quad \varphi_2^{\mathbf{F_{2/2}}}(z) = \frac{5}{8}z + \frac{3}{8}z^2;$$
$$C: \quad \varphi_2^{\mathbf{F_{2/2}}}(z) = \frac{7}{8}z + \frac{1}{8}z^2;$$
$$D: \quad \varphi_2^{\mathbf{F_{2/2}}}(z) = \frac{1}{2}z + \frac{1}{2}z^2;$$
$$E: \quad \varphi_2^{\mathbf{F_{2/2}}}(z) = z.$$

Using these generating functions we have performed calculations for the boxes $\mathbf{F}_{64/384}$ and get the results shown in Figure 7. We have also performed statistic experiments that proved the theoretic calculations. The same results we have also got for the box $\mathbf{F}^{-1}_{64/384}$. This is explained by the mirror-symmetry topology of the boxes $\mathbf{F}_{64/384}$ and $\mathbf{F}^{-1}_{64/384}$.

3 Eagle-128: A New Block Cipher Design

The proposed cipher design, Eagle-128, is based on the combination of CSPNs with SPNs. The CSPNs implements the $\mathbf{F}_{64/384}$ and $\mathbf{F}_{32/32}$ operations built up using the (e,i,g,f) and (e,b,b,c) elements, correspondingly, as standard building block. $\mathbf{F}_{32/32}$ box is implemented as active cascade containing 16 elements $\mathbf{F}_{2/2}$. The (e,i,g,f) element was selected as elementary primitive, since the algebraic degree of its BFs f_1, f_2, and f_3 is equal to 3 (this is maximum possible value for CEs $\mathbf{F}_{2/2}$ satisfying criteria C1 to C4). The outputs of the (e,i,g,f) element are described as follows:

$$y_1 = vzx_2 \oplus vx_2 \oplus vx_1 \oplus zx_1 \oplus z \oplus x_2; \qquad \mathrm{NL}(y_1) = 4;$$

$$y_2 = vzx_1 \oplus vz \oplus vx_2 \oplus zx_1 \oplus zx_2 \oplus x_1; \qquad \mathrm{NL}(y_2) = 4;$$

$$y_1 \oplus y_2 = vzx_1 \oplus vzx_2 \oplus vz \oplus vx_1 \oplus zx_2 \oplus z \oplus x_1 \oplus x_2; \quad \mathrm{NL}(y_1 \oplus y_2) = 4.$$

Table 2: Differential properties of the $\mathbf{F}_{2/2}$ controlled involutions having maximum non-linearity

Average entropy $\overline{\mathrm{H}}$	Number of variants N	Generating subset of 2×2 substitutions	Examples
0.840	128	e, f, g, h, i, j	(e, f, g, h); (f, i, e, j); (h, f, j, e); (j, i, f, e)
0.834	704	a, b, c, d, e, f, g, h, i, j	(a, d, g, i); (b, i, c, h); (f, i, e, h); (j, i, f, d)
0.815	128	a, b, c, d, g, h, i, j	(a, b, j, g); (b, d, h, i); (h, c, i, a); (j, g, c, d)
0.813	192	a, d, e, f, g, h, i, j	(e, e, g, j); (f, h, f, h); (h, h, e, e); (j, f, g, f)
0.812	256	b, c, e, f, g, h, i, j	(b, e, g, h); (c, i, e, j); (e, b, h, j); (i, e, j, e)
0.791	128	e, f, g, h, i, j	(e, g, j, h); (f, h, i, g); (g, h, h, e); (j, i, i, f)
0.788	128	b, c, e, f, h, h, i, j	(b, g, h, e); (c, h, j, f); (h, e, c, g); (j, f, b, i)
0.786	64	e, f, g, h, i, j	(e, g, h, f); (g, f, f, i); (i, e, e, j); (j, f, e, h)
0.774	32	g, h, i, j	(g, g, h, i); (h, i, j, j); (i, j, h, j); (j, i, j, h)
0.731	32	g, h, i, j	(g, g, h, h); (h, g, i, j); (i, g, i, g); (j, g, i, h)
0.719	96	a, b, c, d, e, f, g, h, i, j	(a, g, g, d); (b, h, i, c); (h, c, b, h); (j, f, e, g)
0.710	16	g, h, i, j	(f, h, e, i); (h, j, j, i); (i, g, j, i); (j, i, i, g)
0.695	192	a, b, c, d, e, f, g, h, i, j	(a, b, e, e); (d, f, c, e); (g, d, c, g); (j, c, d, j)
0.641	32	e, f, g, h, i, j	(e, h, i, e); (f, g, g, f); (h, e, e, i); (j, f, f, g)
0.631	64	a, b, c, d, e, f	(a, e, e, b); (c, e, f, a); (e, c, a, f); (f, d, c, f)
0.513	16	g, h, i, j	(g, h, h, g); (h, g, j, i); (i, g, g, i); (j, i, h, g)

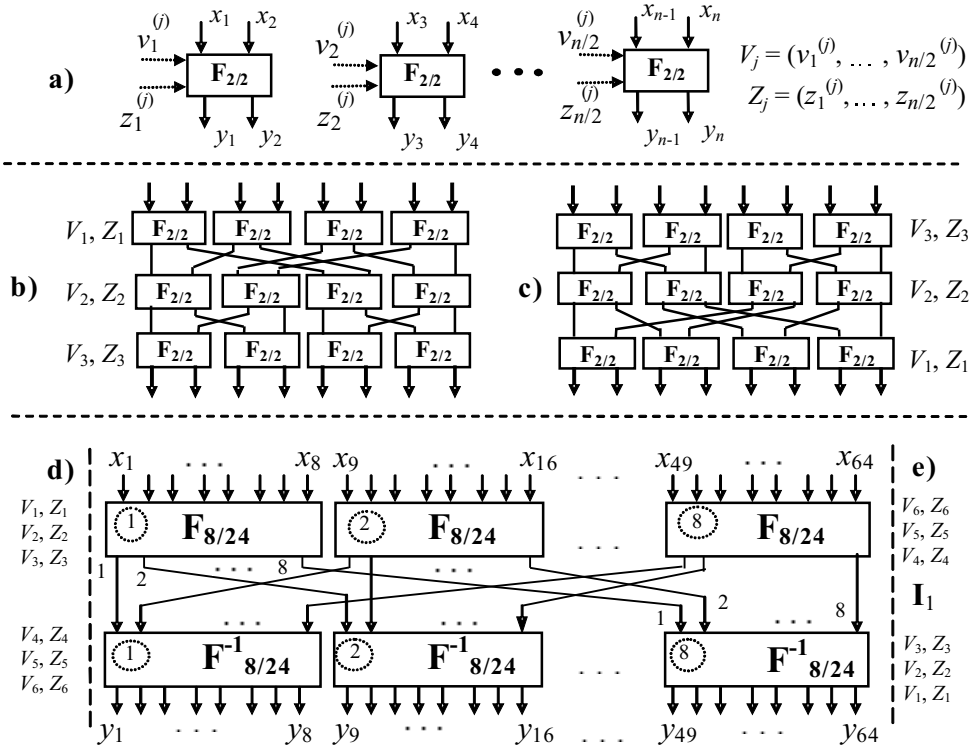


Figure 6: Topology of the DDO boxes: a - one active cascade ($\mathbf{F}_{n/n}$); b - $\mathbf{F}_{8/24}$, c - $\mathbf{F}^{-1}_{8/24}$, d - $\mathbf{F}_{64/384}$, and e - $\mathbf{F}^{-1}_{64/384}$

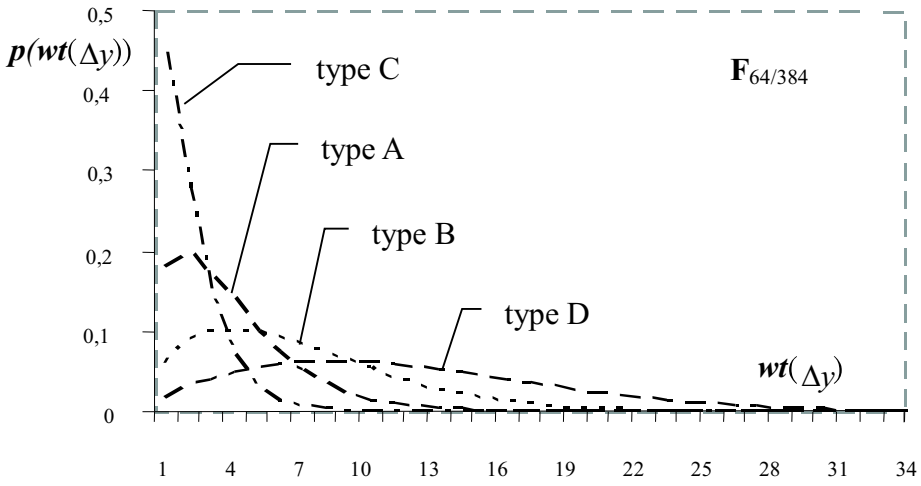


Figure 7: Dependence $p(wt(\Delta y)/wt(\Delta x) = 1, wt(\Delta v, \Delta z) = 0)$ for the $\mathbf{F}_{64/384}$ boxes of different types

The (e,b,b,c) elements has been selected to strengthen the diffusion property of the $\mathbf{F}_{32/32}$ box. This type of CEs is described by the BFs:

$$y_1 = vzx_1 \oplus vzx_2 \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus zx_2 \oplus z \oplus v \oplus x_2; \quad \mathrm{NL}(y_1) = 2;$$

$$y_2 = vzx_1 \oplus vzx_2 \oplus vz \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus zx_2 \oplus x_1; \quad \mathrm{NL}(y_2) = 2;$$

$$y_3 = vz \oplus v \oplus z \oplus x_1 \oplus x_2; \quad \mathrm{NL}(y_3) = 4;$$

A single active bit at the controlling input of the $\mathbf{F}_{32/32}$ box causes generation of one or two active bits at the output (each of these two events has probability 0.5). Both the iterative structure and the round transformation (procedure **Crypt**) of Eagle-128 are presented in Figure 8. Two mutually inverse SPNs used in the right branch are specified in Figure 9, where the 4×4 substitutions $S_0, \ldots, S_7$ are specified in Table 3 (specification of the $S_0^{-1}, \ldots, S_7^{-1}$ boxes can be easily derived from this table). Eight 4×4 S-boxes of the DES cipher (one from each of eight 6×4 S-boxes) have been selected, as the $S_0, \ldots, S_7$ boxes of Eagle-128 in order to inspire a high level of public confidence that no trapdoor are inserted. Similar justification of the S-boxes selection has been earlier used in the design of the Serpent cipher [1]. The permutation I_0 is described as follows:

$$(1)(2, 34)\ldots(2i-1)(2j, 2j+32)\ldots(63)(32, 64),$$

where $i = 1, 2, \ldots, 32$ and $j = 1, 2, \ldots, 16$.

Subkeys $K_i \in \{0,1\}^{64}$ of the 256-bit secret key $K = (K_1, K_2, K_3, K_4)$ are used directly in procedure **Crypt** as round keys Q_j (encryption) or Q'_j (decryption) specified in Table 4. Thus, no preprocessing the secret key is used. More over, in each round transformation we use only one 64-bit subkey combined with both the left and the right data subblocks. This makes the hardware implementation to be cheaper. Procedure **Crypt** is not involution, its part after combining the round key with data subblocks is involution though. In order to symmetries the full ciphering procedure we use very simple final transformation (FT) that is XORing a subkey with both data subblocks. Due to FT in Eagle-128 the same algorithm performs both the encryption and the decryption, while different key scheduling is used.

The 192-bit controlling vectors V and V' corresponding to the $\mathbf{F}_{64/192}$ and $\mathbf{F}^{-1}_{64/192}$ boxes are formed with the extension box $\mathbf{E}$ described as follows:

$$\mathbf{E}(X) = V = (V_1, Z_1, V_2, Z_2, V_3, Z_3);$$

$$V_i = X^{>>>10(i-1)}; \quad Z_i = X^{>>>10i-5}; i = 1, 2, 3,$$

where $X^{>>>b}$ denotes cyclic rotation of the word $X = (x_1, \ldots, x_{32})$ by b bits, i. e. $\forall i \in \{1, \ldots, 32-k\}$ we have $y_i = x_{i+k}$ and $\forall i \in \{33-k, \ldots, 32\}$ we have $y_i = x_{i+k-32}$. The 32-bit controlling vector (V_1, Z_1) of the $\mathbf{F}_{32/32}$ operation is described as follows: $V_1 = (x_1, \ldots, x_{16})$ and $Z_1 = (x_{17}, \ldots, x_{32})$.

The encryption process of Eagle-128 is described as follows:

1) For $j = 1$ to 9 do: $\{(L, R) \leftarrow \mathbf{Crypt}^{(e)}(L, R, Q_j); (L, R) \leftarrow (R, L)\}$.

2) Perform transformation: $\{(L, R) \leftarrow \mathbf{Crypt}^{(e)}(L, R, Q_{10})\}$.

3) Perform final transformation: $\{(L, R) \leftarrow (L \oplus Q_{11}, R \oplus Q_{11})\}$.

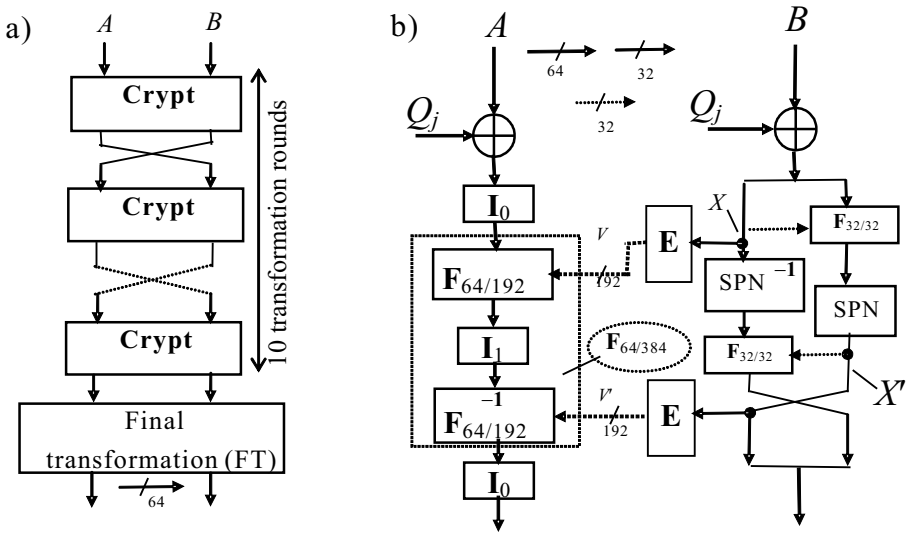


Figure 8: Iterative structure of Eagle-128 (a) and design of procedure Crypt (b)

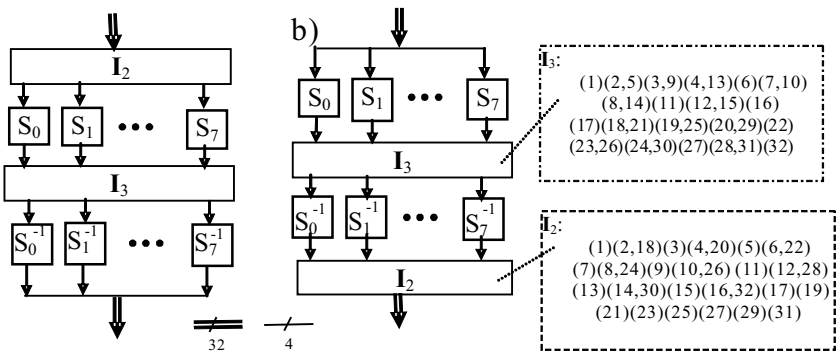


Figure 9: Design of mutually inverse operations SPN (a) and SPN^{-1} (b)

Table 3: Specification of the 4×4 substitution boxes $S_0, \ldots, S_7$

S_0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
S_1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
S_2	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
S_3	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
S_4	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
S_5	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
S_7	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2

Table 4: The key scheduling in Eagle-128 ($j = 11$ corresponds to final transformation)

Round number $j =$	1	2	3	4	5	6	7	8	9	10	11
Encryption $Q_j =$	K_1	K_2	K_3	K_4	K_2	K_1	K_3	K_4	K_3	K_2	K_1
Decryption $Q'_j =$	K_1	K_2	K_3	K_4	K_3	K_1	K_2	K_4	K_3	K_2	K_1

4 VLSI Synthesis Results & Comparisons

The proposed DDP-based block cipher, Eagle-128, has been proven as an efficient design with low hardware implementation cost. Security estimations [7, 8, 9] of DDP-based ciphers have shown that DDP boxes, combined with some additional operations having comparatively low non-linearity, can thwart well both linear and differential analysis. Both the FPGA and the ASIC implementations synthesis results [14, 15, 16] prove that DDP-based ciphers provide high performance, with less allocated hardware resources.

Because of linearity of the $\mathbf{P}_{2/1}$ element (for which we have $\mathrm{NL}(f_1) = \mathrm{NL}(f_2) = 2$ and $\mathrm{NL}(f_3) = 0$) the DDP boxes are linear cryptographic operations, (implemented using the switching element as main building block). Another peculiarity of the DDP boxes, which restricts the efficiency of the DDP-based design, consists in that no avalanche is introduced while inverting a bit at the input of the DDP operation. The DDP contributes the avalanche only while inverting bits at the controlling input. Taking into account these disadvantages, we have proposed a new class CEs providing the design of the advanced DDO boxes that are non-linear operations, contributing significantly while complementing bits at both the input and the controlling input. More over, new DDO operations and DDP constructed using the same numbers of CEs are implemented in the FPGAs devices, using the same number of Configurable Logic Blocks (CLBs), and in the ASIC devices, using approximately the same number of logic gates.

Replacing the switching elements $\mathbf{P}_{2/1}$ by CEs $\mathbf{F}_{2/2}$ in the linear DDP boxes (a number of which are considered in [6, 16]), we get non-linear DDO boxes with significantly advanced contribution to the avalanche. This improvement does not increase the cost, for a hardware implementation. Due to advanced cryptographic properties the $\mathbf{F}_{64/384}$ and $\mathbf{F}^{-1}_{64/384}$ boxes can be efficiently used for the design of DDO-based ciphers.

For example, the replacement of DDP boxes by the proposed DDOs, having the same input size, in the known DDP-based ciphers [6, 15, 16] yields secure reduction of rounds, providing higher performance for the loop architecture or lower cost for the pipeline architecture. In the known DDP-based iterative ciphers the round transformation does not change one of data subblocks, or performs on it only fixed bit permutation. This imposes certain restrictions on increasing "performance per cost" value. In Eagle-128 we have used an advanced cryptoscheme providing transformation of both the left and the right data subblocks, the time delay of one round being significantly reduced. This cipher extensively uses the property of controllability of the used operations.

We have implemented Eagle-128 using both ASIC (0.33 um) and FPGA (Xilinx Virtex) technologies. For both implementations a typical loop unrolling architecture is used. Denoted as LU-N, where N is number of the unrolled encryption rounds [4]; the iterative looping architecture corresponds to LU-1. This type of architecture has been selected to perform comparisons, since it suits well to implementation of the CBC (Cipher Block Chaining) encryption mode. Due to the use of the FPGA-oriented primitives the Eagle-128 is significantly more efficient for the FPGA implementation against majority of the known 64-bit block ciphers (for example, 3-DES [12], IDEA [2]) including the DDP-based ones (Cobra-H64 [16], CIKS-1 and SPECTR-H64 [14]). The Eagle-128 is also more efficient than the 128-bit block ciphers including AES finalists (Rijndael, Serpent, RC6, and Twofish) and DDP-based ones (Cobra-H128 [16] and SPECTR-128 [6]). In Table 5, comparisons of the FPGA implementations efficiency are presented (Performance/Cost and Performance/(Cost* Frequency)) of Eagle-128 with other well known block ciphers.

In addition, two comparison models, Performance/Area and Performance/(Area*Frequency), are used. It is obvious that the proposed applied methodology of Eagle-128 achieves higher throughput values. It also covers significant less area resources than other 128-bit ciphers, for an FPGA LU-N architecture implementation. The Performance/Area ratio and Performance/(Area* Frequency) ratio comparisons indicate that the proposed Eagle-128 is also significantly better compared with different designs of 64-bit ciphers for the both comparison models, except the 64-bit cipher DES [12].

5 Security Estimation

Investigation of statistic properties of Eagle-128 has been carried out with standard tests, which have been used in [11] for testing five AES finalists. Our research results have shown that three rounds of Eagle-128 are sufficient to satisfy the test criteria. Thus, Eagle-128 possesses good statistical properties like that of AES finalists. Our preliminary security estimation of Eagle-128 shows that its four (eight) rounds are sufficient to thwart linear (differential) attack. Similarly to earlier results on analysis of the DDP-based ciphers [7, 8, 9] the differential attack against Eagle-128 is more efficient than linear one. The best iterative differential characteristics are presented in Table 6, where (Δ^A_h, Δ^B_z) and (δ^A_h, δ^B_z) denote input and output differences, respectively. Formation scheme of the characteristic corresponding to the difference (Δ^A_2, Δ^B_0) is presented in Appendix (Figure 10). Each difference is represented as concatenation two differences corresponding to the A and B data subblocks. Indices h and z indicates the number of active (non-zero) bits. Note that Δ^W_h denotes any possible difference with h active bits in the W data subblock. Probability that the difference (Δ^A_h, Δ^B_z) passes r rounds and transforms into the difference (δ^A_h, δ^B_z) is denoted as $P(r)$.

Probability to have at output of the random cipher the

Table 5: LU-N architectures: VLSI implementations comparisons

BLOCK CIPHERS	Block Size (bit)	Rounds	N	Area, (CLBs)	F (MHz)	Rate (Mbps)	Integral efficacy	
							Mbps/ CLBs	Mbps/ (CLBs*GHz)
Eagle-128 (FPGA) Proposed	128	10	1	781	92	1,177	1.51	16.4
Eagle-128 (FPGA) Proposed ♢	128	10	♢	4,120	95	12,160	2.9	30.5
Eagle-128 (ASIC) Proposed	128	10	1	3,104 sqmil	110	1,408	0.45 Mbps/sqmil	4.9 Mbps (sqmil*GHz)
Eagle-128 (ASIC) Proposed ♢	128	10	♢	16,780 sqmil	112	14,336	0.85 Mbps/sqmil	7.6 Mbps/ (sqmil*GHz)
Cobra-H128 [16]	128	12	1	2,364	86	917	0.39	4.5
Cobra-H128 (ASIC) [16]	128	12	1	6,364 sqmil	90	1,000	0.16 Mbps/sqmil	1.78 Mbps/ (sqmil*GHz)
Rijndael [14]	128	10	1	2,358	22	259	0.11	5.0
Rijndael [4]	128	10	1	3,528	25.3	294	0.083	3.3
Rijndael [4]	128	10	2	5,302	14.1	300	0.057	4.4
Rijndael [3]	128	10	1	3,552	54	493	0.138	2.56
Rijndael [12]	128	10	-	2,257	127	1,563	0.69	5.4
Rijndael [13]	128	10	-	256K gates	32	7,500	0.029 Mbps/gate	0.91 Mbps/ (gate*GHz)
Serpent [4]	128	32	8	7,964	13.9	444	0.056	4.0
RC6 [4]	128	20	1	2,638	13.8	88.5	0.034	2.4
Twofish [4]	128	16	1	2,666	13	104	0.039	3.0
Cobra-H64 [16]	64	10	1	615	82	525	0.85	10.4
Cobra-H64 (ASIC) [16]	64	10	1	2694 sqmil	100	640	0.20 Mbps/sqmil	2.0 (sqmil*GHz)
SPECTR-H64 [14]	64	12	1	713	83	443	0.62	7.5
CIKS-1 [14]	64	8	1	907	81	648	0.71	8.9
DES [12]	64	16	-	189	176	626	3.21	18.2
3-DES [12]	64	3×16	-	604	165	587	0.94	5.7
IDEA [2]	64	8	1	2,878	150	600	0.28	1.87

where rows marked with ♢ present results on the pipeline implementation architecture

Table 6: The best differential characteristics of Eagle-128

Input difference	Output difference	r	$P(r)$
(Δ_2^A, Δ_0^B)	(δ_4^A, δ_0^B)	2	$\approx 2^{-38.5}$
(Δ_4^A, Δ_0^B)	(δ_2^A, δ_0^B)	2	$\approx 2^{-39}$
(Δ_2^A, Δ_0^B)	(δ_2^A, δ_0^B)	2	$\approx 2^{-36.5}$
(Δ_2^A, Δ_0^B)	(δ_2^A, δ_0^B)	4	$\approx 2^{-73}$
(Δ_2^A, Δ_0^B)	(δ_2^A, δ_0^B)	6	$\approx 2^{-109.5}$
(Δ_2^A, Δ_0^B)	(δ_2^A, δ_0^B)	8	$\approx 2^{-139}$
(Δ_2^A, Δ_0^B)	(δ_0^A, δ_2^B)	10	$\approx 2^{-170}$

difference (δ_2^A, δ_0^B) is equal to $P_{rand} > 2^{-115} > P(8) > 2^{-147}$. Thus, the cipher Eagle-128 with eight encryption rounds appears to be indistinguishable from a random cipher with the most efficient differential characteristics.

6 Conclusion

This work focuses on advancing the DDO-based approach to the block cipher design. A new class of the $\mathbf{F}_{2/2}$-type CEs have been introduced as cryptographic primitive suitable to the design of the FPGA and ASIC efficient DDO boxes. The full classification of the DCs have been performed for the $\mathbf{F}_{2/2}$ CEs having maximum non-linearity $\mathrm{NL}(f_1) = \mathrm{NL}(f_2) = \mathrm{NL}(f_3) = 4$.

Using new DDO boxes a new 128-bit block cipher named Eagle-128 that is efficient for application in the constrained environments has been proposed. The VLSI implementation of Eagle-128 is well suited in the cases while restricted FPGA or ASIC resources are available for embedded cryptographic modules. Hardware efficiency of Eagle-128 is provided by i) the use of the advanced $\mathbf{F}_{2/2}$ CEs and ii) combining the CSPNs with SPNs in the round transformation. The second element of the new cipher design provides simultaneous transformation of the both data subblocks and can be also applied in the case of DDP-based ciphers, probably while ASIC implementation where the DDP boxes are a bit more efficient and fast. However comparison with the known DDP-based designs shows the new DDO-based cipher is more efficient for both the FPGA and the ASIC implementation.

References

[1] R. Anderson, E. Biham, and L. Knudsen, "Serpent: a proposal for the advanced encryption standard," in *1st Advanced Encryption Standard Candidate Conference Proceedings*, Venture, California, Aug. 20-22, 1998.

[2] O. Y. H. Cheung, K. H. Tsoi, P. H. W. Leong, and M. P. Leong, "Tradeoffs in parallel and serial implementations of the international data encryption algorithm," in *Proceedings of the 3rd International Workshop Cryptographic Hardware and Embedded Systems - CHES 2001*, LNCS 2162, pp. 333-347, Springer-Verlag, 2001.

[3] C. Chitu, and M. Glesner, "An FPGA implementation of the AES-Rijndael in OCB/ECB modes of operation," *Microelectronics Journal, Elsevier Science*, vol. 36, pp. 139-146, 2005.

[4] A. J. Elbirt, W. Yip, B. Ghetwynd, C. Paar, "FPGA implementation and performance evaluation of the AES block cipher candidate algorithm finalists," in *3rd Advanced Encryption Standard Conference Proceedings*, New York, NY, USA (http://www.nist.gov/aes), Apr. 13-14, 2000.

[5] M. A. Eremeev, A. A. Moldovyan, and N. A. Moldovyan, "Data encryption transformations based on new primitive," *Avtomatika i Telemehanika (Russian Academy of Sciences)*, no. 12, pp. 35-47, 2002.

[6] N. D. Goots, et al, *Modern cryptography: Protect Your Data with Fast Block Ciphers*, Wayne, A-LIST Publishing, 2003. (www.alistpublishing.com).

[7] N. D. Goots, et al., "Fast ciphers for cheap hardware: differential analysis of SPECTR-H64" in *Proceedings of the International Workshop, Methods, Models, and Architectures for Network Security*, LNCS 2776, pp. 449-452, Springer-Verlag, 2003.

[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 International Workshop, Methods, Models, and Architectures for Network Security*, LNCS 2776, Springer-Verlag, 2003.

[9] Ch. Lee, D. Hong, Sun. Lee, San. Lee, S. Yang, and J. Lim, "A chosen plaintext linear attack on block cipher CIKS-1," in *Proceedings of the 4th International Conference on Information and Communications Security*, LNCS 2513, pp. 456-468, Springer-Verlag, 2002.

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

[11] B. Preneel et al., *Comments by the NESSIE project on the AES finalists*, May 24, 2000 (http://www.nist.gav/aes).

[12] B. Preneel et al., *Performance of Optimized Implementations of the NESSIE Primitives*, project IST-1999-12324, 2003. (see pp. 36; http://www.cryptonessie.org).

[13] A. Rudra, P. K. Dubey, C. S. Jutla, V. Rumar, J. R. Rao, and P. Rohatgi, "Efficient Rijndael encryption implementation with composite field arithmetic," in *Proceedings of the 3rd International Workshop Cryptographic Hardware and Embedded Systems - CHES 2001*, LNCS 2162, pp. 171-180, Springer-Verlag, 2001.

[14] N. Sklavos et al, "Encryption and data dependent permutations: implementation cost and performance evaluation," in *Proceedings of the International Workshop, Methods, Models, and Architectures for Network Security*, LCNS 2776, pp. 337-348, Springer-Verlag, 2003.

[15] N. Sklavos and O. Koufopavlou, "Architectures and FPGA implementations of the SCO (-1,-2,-3) ciphers family," in *Proceedings of the 12th International Conference on Very Large Scale Integration, (IFIP VLSI SOC '03)*, Darmstadt, Germany, Dec. 1-3, 2003.

[16] 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, Kluwer Academic Publishers*, vol. 25, no. 1-2, pp. 219-231, 2005.

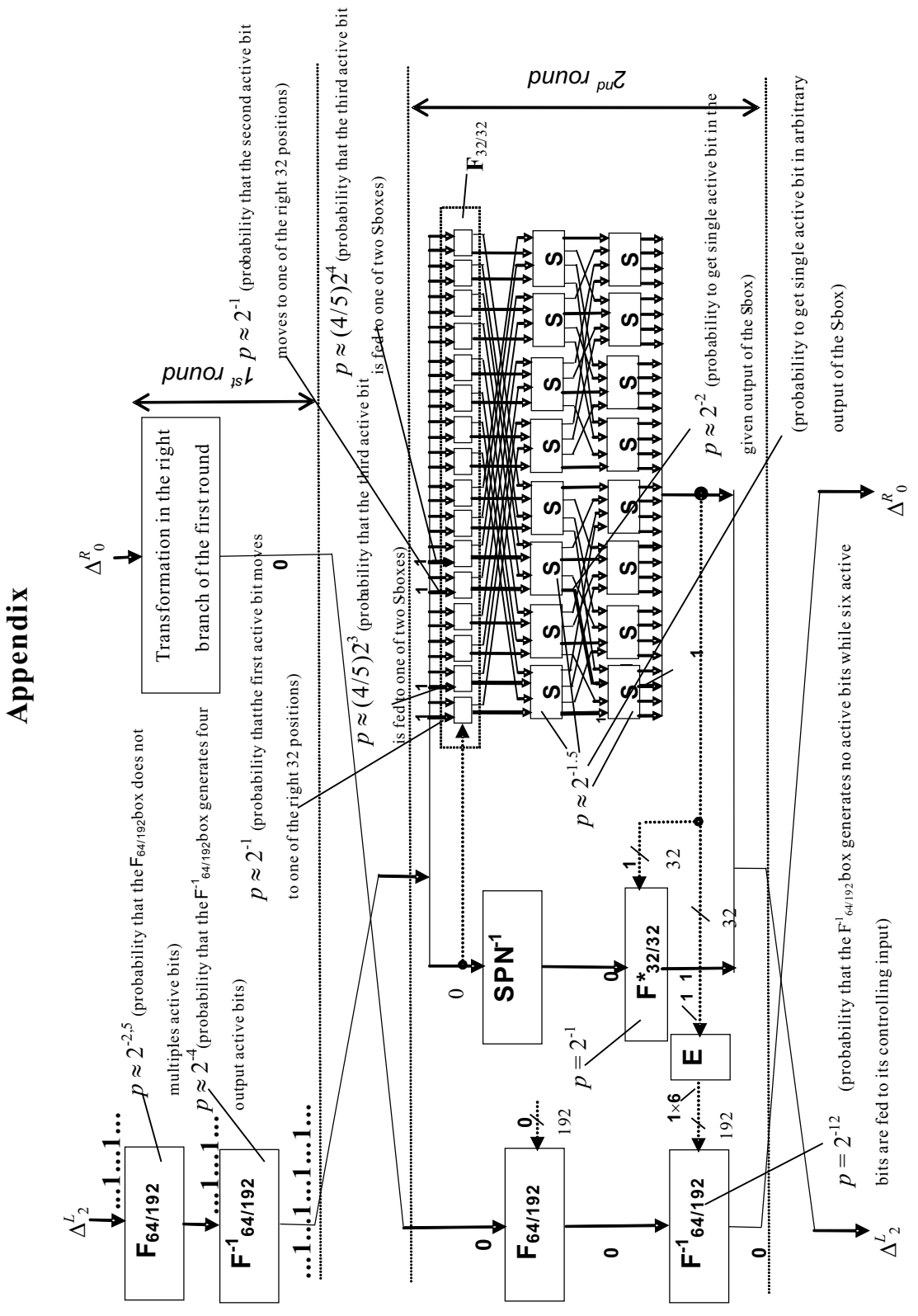
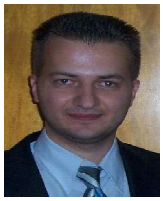


Figure 10: Formation of the two-round iterative difference (Δ_2^L, Δ_0^R) with probability P(2)$\approx 2^{-36,5}$

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.



Nicolas Sklavos received the Ph.D. Degree in Electrical & Computer Engineering, and the Diploma in Electrical & Computer Engineering, in 2004 and in 2000 respectively, both from the Electrical & Computer Engineering Dept., University of Patras, Greece. His research interests include Cryptography, Wireless Communications Security, Computer Networks and VLSI Design. He holds an award for his PhD thesis on "VLSI Designs of Wireless Communications Security Systems", from IFIP VLSI SOC 2003. He has participated to international journals and conferences organization, as Program Committee Member and Guest Editor. Dr. N. Sklavos is a member of the IEEE, the Technical Chamber of Greece, and the Greek Electrical Engineering Society. He has authored or co-authored more than 80 scientific articles, books chapters, tutorials and reports, in the areas of his research. Contact him at: nsklavos@ieee.org.